

## Sosyal Medyanın Bilgi Kalitesine Etkisi: Sahte Hesaplar

Hilal UZUN<sup>1</sup>

<sup>1</sup>Hacettepe Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü, Ankara  
h.uzun10@hacettepe.edu.tr

### ÖZET

*İletişim, insanlar ve topluluklar için hayatın vazgeçilmez bir faaliyetidir. İnsanın öğrenme ve bilme ihtiyacı sonucu ortaya çıkan merak duygusu çevresindeki olaylardan haberdar olma isteği, sosyalleşme isteği iletişim kurmasının nedenleri arasında sayılabilir. Hızla gelişen teknoloji, iletişim araçlarının ve ortamlarının değişmesini neden olmuştur. 20. yüzyılın en büyük olayı internetin bulunmasıdır. Bilgisayar teknolojileri ve internet insanların iletişim ve bilgi edinme davranışlarını değiştirmiş, bilgi çağı kavramının ortaya çıkmasına neden olmuştur. Yapılan araştırmalar göstermektedir ki biz ve bizden sonraki nesiller giderek teknolojiye daha bağımlı hale gelmekteyiz. Bilgiyi hızlıca sunan ve yayan mecralar bilgi verme ve alma araçları haline gelmektedir. Bu araçlardan en bilinenleri de sosyal medya araçlarıdır. Çünkü sosyal medya araçları insanları etkileşimde bulunmaya, tartışmaya, bildiklerini söylemeye, katılmaya teşvik eder. Aslında sosyal medyada içeriği kullanıcılar oluşturur. İnsanlara sanal ortamda özgürce davranma hakkı sunması sebebiyle popülerliğini giderek artmaktadır. Sosyal medyanın bilgi yaymak ve toplamak için kullanımının giderek artması ile bu alandaki bilgilerin doğrulanması sorunu da artmaktadır. Herhangi bir denetim mekanizması bulunmayan sosyal medya artık bilgi çöplüğüne dönüştü diyebiliriz. Bunun pek çok nedeni vardır ancak bu çalışmada ele alınan nokta "sahte hesaplar". Sosyal alanlarda bir kişi istediği takdirde istediği kadar hesap açabilir ve kimliğini belirtmek zorunda değildir. Bu çalışma sahte hesapları tespit eden araçların yeterliliklerini değerlendirmek amacıyla gerçekleştirilmiştir. Çalışmada Facebook, Twitter, Instagram gibi sosyal paylaşım sitelerine yönelik hazırlanmış online sahte hesap tespit araçları ile uygulama yapılarak sonuçlar değerlendirilmiştir. Elde edilen sonuçlara göre, sahte hesapları tespit etmek için geliştirilen çevrimiçi uygulamaların yeterli olmadığı görülmektedir.*

**Anahtar Kelimeler: Sosyal ağlar, sahte hesap, bot hesap, sahte hesap bulma araçları**

### Impact of Social Media on Knowledge Quality: Fake Accounts

### ABSTRACT

*Communication is an indispensable activity for people and communities. The desire to be aware of the events surrounding the sensation of curiosity that has emerged as a result of the need for learning and knowing can be considered as one of the reasons for communicating the desire for socialization. Rapidly evolving technology has caused communication tools and environments*

*to change. The greatest event of the 20th century is the Internet. Computer technology and the Internet have changed people's behavior of communication and information, leading to the emergence of an information age concept. Research shows that we and the next generations are increasingly becoming more dependent on technology. Rapidly presenting and disseminating information becomes a means of providing and receiving information. The most popular of these tools are social media tools. Because social media tools encourage people to interact, discuss, say what they know, participate in. It actually creates content users in the social media. Its popularity is steadily increasing because it offers people the right to behave freely in the virtual environment. The increasing use of social media to disseminate and collect information and the problem of verifying this information is also increasing. We can say that social media, which does not have any control mechanism, has turned into information garbage. There are many reasons for this, but the point that is addressed in this study is "fake accounts". In social areas, a person can open as many accounts as he or she desires and do not have to specify their identity. This study was conducted to evaluate the adequacy of the tools that detect forged accounts. In the study, results were evaluated by using online forged account identification tools prepared for social sharing sites like Facebook, Twitter and Instagram. According to the results obtained, online applications developed to detect fake accounts are not enough.*

**Keywords: Social networks, fake account, bot account, fake account finder**

## GİRİŞ

### Konunun Önemi

Karşılıklı ve eş zamanlı iletişime imkân sağlayan, hızlı ve ucuz olması açısından avantajlı olan sosyal medyanın kullanımı giderek artmaktadır. Ancak doğru bilgiye erişmek isteyen ve doğru bilgiye erişirmekle sorumlu olan bilgi profesyonelleri olarak dikkat çekmemiz gereken husus; giderek kullanımı artan, denetim-kontrol-doğrulama mekanizması olmayan sosyal medyada bilgi havuzu ne durumdadır? Bilgiyi sosyal medyada paylaşan kişi gerçekten o bilgiye sahip midir? Bilgiyi nereden elde etmiş? Nasıl analiz etmiştir? Bunlar sosyal medyada bilgiyle karşılaştığımızda aklımıza gelen sorulardır. Esas nokta bilginin sunuş ortamından çok kim tarafından sunulduğu sorudur. Çünkü günümüzde sosyal alanlarda insanlar kimliklerini gizleyebilmektedirler. Sanal ortamlarda kimliğini saklayarak gezinme insanlardaki sorumluluk duygusunu azaltır. Ancak bu durum ilerleyen zamanlarda farklı sonuçlar doğurabilmektedir. Kendi kimliğini saklarken bir başkasını taklit etme ya da olduğundan farklı görünmek için bot hesaplar satın alma gibi olaylar her geçen gün giderek artmaktadır. Kim olduğunu bilmediğimiz ya da aslında başkasını taklit eden bu kişiler sosyal mecraların iletişim gücünden faydalanarak yanlış ve eksik bilgiler yayabilir. Örneğin; Türkiye’de Gezi Parkı Protestoları olduğu sırada Twitter’da

ismini saklayan biri “Ankara Güvenpark’ta polis insanlara ilaçlı su vererek bayıltıp sessizce gözaltına alıyor, kimse tanımadığı kişilerden su almasın” diye bir tweet attı diyelim bu durumda ne yaparsınız? Burada önemli bir bilgi var buna inanmayı mı seçeceksiniz yoksa yalan olduğunu mu düşüneceksiniz? Ya da bu tweet’i atan kişiye mi ulaşmaya çalışacaksınız? Bu tweet’i atan kişi böyle bir olayı bizzat yaşadı mı ya da kendi tanık olduğu bir olay mı var? İşte bunların hepsinin cevabını bulabilmek için öncelikle o tweet’i atan hesabın sahibini bulmanız gerekir. O kişi belki de hiç Ankara’da bulunmamış biri olabilir, kötü niyetle insanları polisle çatıştırmak için tartışma başlatmaya çalışıyor olabilir. Ya da gerçekten böyle bir olayı gördüğü için iyi niyetle uyararak da istemiş olabilir. Burada kilit nokta o kişinin kimliğini doğrulamak. İşte bu gibi durumlarda bilgiyi doğrulamak için bilginin kaynağı olan hesapların doğruluğundan emin olmalıyız. Bu yüzden sahte hesapları nasıl tespit edebileceğimizi bilmek çok önemlidir. Dünya da giderek bunun farkına varmakta ve sahte hesapların önüne geçmek için çeşitli çalışmalar yapmaya başlamıştır. Instagram, Twitter, Facebook gibi sosyal ağlar sahte hesap temizliğine girişerek tespit ettikleri milyonlarca sahte hesabı temizlemektedir. Bununla ilgili sosyal ağ siteleri her ne kadar temizlik işine girişeler de sosyal ağ kullanıcıları olarak bizim de bu konuda bilgi sahibi olmamız lazım ki kendimizi ve çevremizi sahte hesaplardan gelen bilgi kirliliğine karşı koruyabilelim.

### **Araştırmanın Amacı**

Bu araştırmanın temel amacı; sosyal mecralarda yayılan bilgileri incelerken bilgi sağlayıcısı olan kaynakların doğrulanması gerekliliğinin önemi üzerindedir. Bununla ilgili olan terimler (sahte hesap, bot hesap) açıklanarak, sahte hesapların tespit edilmesi için geliştirilmiş olan uygulamalar ele alınarak bunların üstüne nasıl gelişmeler yapılabileceği üzerine önerilerde bulunulması hedeflenmiştir.

Bu araştırmada aşağıdaki sorular yanıtlanmaya çalışılacaktır:

- Sahte hesap nedir?
- Neden sahte hesap kullanılır?
- Sahte hesapların bilgi kirliliğine etkisi nedir?
- Sahte hesaplar nasıl anlaşılır?
- Sahte hesaplara karşı neler yapabiliriz?
- Sahte hesapları yakalamak için kullanabileceğimiz çevrimiçi araçlar/siteler nelerdir?
- Sahte hesapları yakalamak için geliştirilmiş çevrimiçi araçlar yeterli midir?

## **Araştırmanın Kapsamı**

Bu araştırma çoğunlukla Twitter, Facebook, Instagram gibi sosyal paylaşım ağlarındaki hesapları kapsamaktadır. Evren olarak da bu ağlardaki hesapları nitelendirebiliriz. Sosyal medya kullanımıyla ilgili verilere baktığımızda bu alanlarda insanların bilgi paylaşımında ve etkileşimde daha çok bulunduğu gözlemlendiği için evren olarak bu ağlar seçilmiştir. Evrenin tam sayısını belirtmek çok güçtür çünkü bu ağ kayıtları 7/24 açıktır, araştırmayı yaparken pek çok hesap silinmiş ya da yeni hesaplar kayıt edilmiş olabilir. Uygulama kısmında bu ağlardan rastgele seçilmiş hesaplar kullanılmıştır. Bu hesapları çoğunlukla kendi çevremden seçtiğim ve sayı olarak az olduğu için örneklem evreni temsil etmemektedir. Ancak durumla ilgili fikir sahibi olmayı sağlayacaktır.

## **Araştırmanın Yöntemi**

Araştırmada betimleme yöntemi kullanılmıştır. Türk Dil Kurumu sözlüğüne göre betimleme; “bir şeyi sözle veya yazıyla anlatma, tasvir” olarak açıklanmaktadır. Betimleme yönetimi çoğunlukla var olan problemi anlama ve anlatmak istenen durumlarda kullanılan bir araştırma yöntemidir. Betimleme yöntemi ile araştırmadaki problemle ilgili durum nedir, ne yapmak istiyoruz, ne yapmalıyız gibi sorulara cevap aranmıştır.

## **Veri Toplama Teknikleri**

Veriler çalışma kapsamı olarak belirlenmiş olan sosyal ağlardan herkese açık olan hesap profilleri içinden bazen bilindik bazen de rastgele olan hesaplardan toplanmıştır.

## **Değerlendirme Teknikleri**

Verileri değerlendirmek için sosyal ağ hesapları hakkında analizler yapan bazı çevrimiçi kaynak doğrulama araçları kullanılmıştır. Bu araçlarının sonuçlarının yeterliliği ve güvenilirliği üzerinde durulmuştur.

## **Kaynaklar**

Sahte hesap problemi güncel bir problem olarak görülmekte ve üzerinde yeni yeni çalışmalara başlanmıştır. Konu ile ilgili daha çok bilişimciler tarafından açılan bilgilendirici blog ve forum siteleri yardımcı olmuştur. Türkiye’de sosyal medyadaki şüpheli bilgileri doğrulama yaparak

okurların gerçek bilgiye ulaşması için çalışan teyit.org topluluğunun çalışmaları araştırmada yol gösterici olmuştur. Özellikle “Doğrulama El Kitabı: Kriz Anlarında Dijital Verilerin Doğrulanması İçin Rehber” kaynağı ana kaynak olmuştur. Araştırmaya yardımcı olan başlıca kaynaklar şunlardır:

- ✓ [https://verificationhandbook.com/book\\_tr/](https://verificationhandbook.com/book_tr/)
- ✓ <https://teyit.org/>
- ✓ <https://wearesocial.com/>
- ✓ <https://gokhanahi.com/>
- ✓ <http://www.hasansabrikayaoglu.com/>
- ✓ <http://usmed.org.tr/> (Uluslararası Sosyal Medya Derneği)
- ✓ Bilgi Teknolojileri ve İletişim Kurumu'nun yayınları

Ayrıca araştırmanın III. bölümünde kullanılan uygulamalar şunlardır:

- ✓ <http://fakers.statuspeople.com/>
- ✓ <https://www.twitteraudit.com/>
- ✓ <http://geosocialfootprint.com/>
- ✓ <https://pipl.com/>
- ✓ <https://www.spokeo.com/>.
- ✓ <http://www.followercheck.co/>

## **KURAMSAL İÇERİK**

### **Sosyal Medya**

Sosyal Medya, bireylerin ve toplulukların ortak içerik oluşturması, paylaşması, tartışması, değiştirmesi için mobil ve web tabanlı teknolojiler ile oluşturulan yüksek etkileşimli platformlar için kullanılan bir terimdir (Vural ve Bat, 2010).

Sosyal medyanın geleneksel medyadan en önemli farklılığı, herhangi bir kişinin sosyal medyada içerik yaratabilmesi, katkı sağlayabilmesidir. Sosyal medya sayesinde bireyler sadece bilgi edinen konumda değil, bilgi sağlayan konumda da bulunmaktadır.

Sosyal medya araçları nelerdir diye bakacak olursak: Facebook, Twitter, Google+, Tumblr, LinkedIn, Youtube, Foursquare, Wordpress(blog), Wikipedia, flickr, Slideshare vb. şeklinde sayılabilir ve bu örnekler çoğaltılabilir. Kısaca içeriğini kullanıcıların oluşturduğu alanlara sosyal medya aracı diyebiliriz. Sosyal medya anlıktır, 24 saat açıktır, zaman ve mekân sınırlandırması vermez.

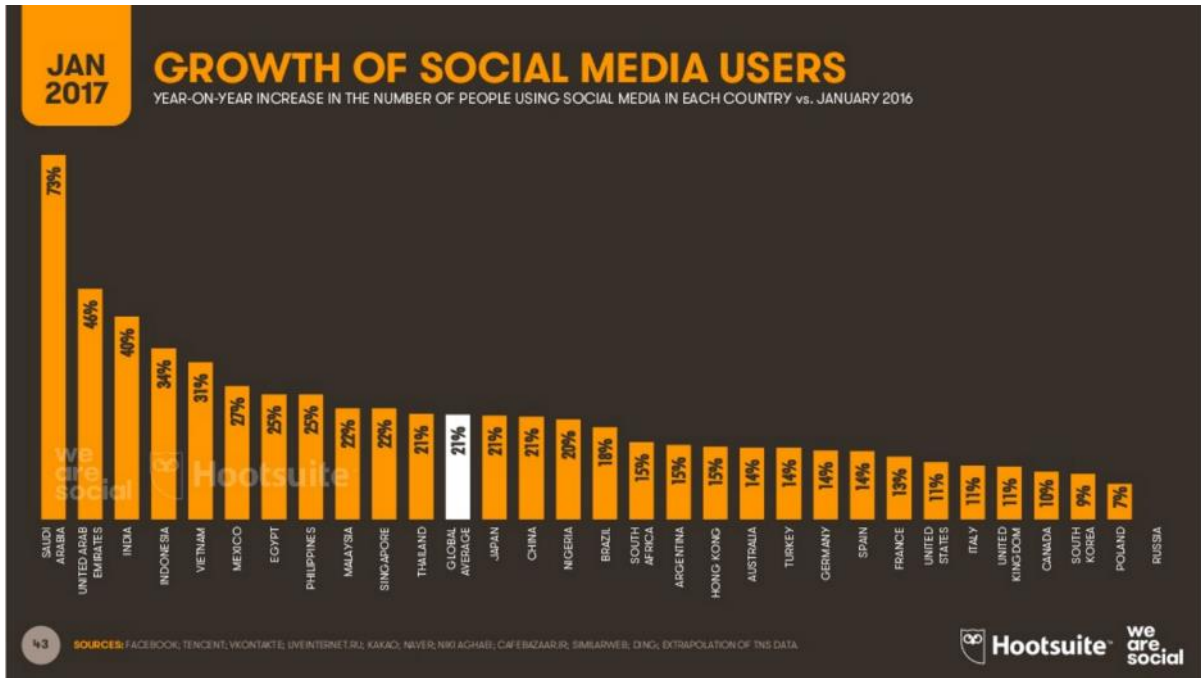
### **Sosyal Medyanın Bilgi Kirliliğine Etkisi**

Geleneksel habercilikte bilginin kim tarafından verildiği yani habercinin kimliği önemli bir husustur. Haberci kimliği ile vereceği haberin doğruluğu arasında bir paralelliğin olduğu düşüncesi hâkimdir. Çünkü haberi veren kişinin isminin belli olması kendisi için bir bağlayıcılık teşkil edeceğinden vereceği haber için de benzer etkiyi bırakacaktır (Genel, 2016). Ancak sosyal medya ortamlarının sağladığı özgürlük ile isteyen kişi kimliğini açıklamadan istediği şekilde bilgi verebilir, bu da ister istemez bilgiye güven sorunlarına neden olmaktadır. Kullanıcılar hiçbir kontrol olmaksızın bir e-posta adresi ile kendi isim veya rumuzlarıyla sosyal mecralara kayıt olarak bilgi üretim ve paylaşımına dâhil olabilmektedir. Basit bir işlemle sosyal ağlara kayıt olan bir kullanıcı, istediği kadar sahte hesap oluşturarak sınırsızca etkileşimde bulunabilmektedir. . Adınıza açılmış sahte bir hesaptan yapılanlar sizin ceza almanıza sebep olabilir ya da sahte bir hesabın verdiği yalan yanlış bilgiler insanları yönlendirip kötü durumlar ortaya çıkmasına neden olabilir.

We Are Social ve Hootsuite tarafından yayınlanan “Digital in 2017: Global Overview” raporu internet, mobil ve sosyal medya kullanıcı istatistikleri hakkında bilgiler veriyor.



Şekil 1: Dünya Dijital Kullanım İstatistikleri

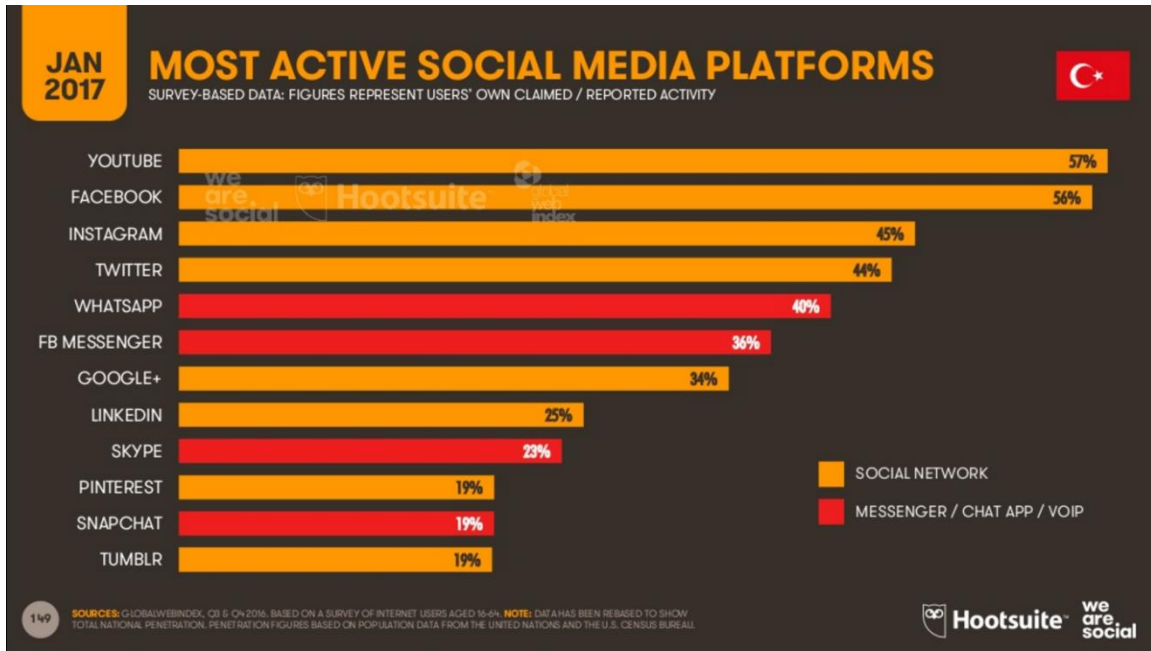


Şekil 2: Sosyal Medya Kullanıcılarının Büyüme Yüzdeleri

Bu istatistiklere göre; dünyada 3.77 milyar küresel internet kullanıcısı ve toplam 2.79 milyar sosyal medya kullanıcı varken, 2.55 milyar mobil sosyal medya kullanıcı mevcut. Aktif sosyal medya kullanıcısı istatistiğine bakıldığında 2015 yılından itibaren ortalama %21'lik bir artış olmuş.



Şekil 3: Türkiye Dijital Kullanım İstatistikleri



Şekil 4: Türkiye’de En Aktif Kullanılan Sosyal Medya Platformları

Türkiye’deki durumu bakarsak:

- Türkiye’de toplam nüfusun %60’lık kesimi yani 48 milyon kişi internet kullanıcısıdır.
- Aktif sosyal medya kullanıcı sayısı olarak da 48 milyonu görüyoruz fakat bu sadece kişilere ait bir sayım değil işletmeler ve markalara ait sosyal ağlar da hesaplanmış.
- Mobil kullanıcı sayısı 71 milyon.



- Sosyal medyaya mobilden bağlanan kullanıcı sayısı 42 milyon.
- En çok kullanılan sosyal medya araçları da sırasıyla: Youtube, Facebook ve Instagram'dır.

Hem ülkemizde hem de dünyada internet kullanımıyla birlikte sosyal ağlardaki aktiflik oranlarının da ciddi şekilde yükseldiğini görmekteyiz. Bu kadar çok insanın bulunduğu sosyal mecralarda bilgi artış hızını ve bu mecraların kontrol-denetim mekanizmalarının olmadığını bilince ortaya büyük ve karmaşık bir bilgi havuzu sorunu çıkıyor.

### **Sahte Hesap**

Günümüzde en popüler haberleşme ve iletişim ortamı sosyal medya alanıdır. İnternet teknolojilerini kullanarak iletişim kurduğumuz, içerik üretebildiğimiz ve bilgi paylaşımı yaptığımız sosyal medya kim olduğunuzu açık bir şekilde belirtmemizi beklemez. Bu durum kişilerin kimliklerini belirtmeden sosyal ağlarda dolaşmalarına ve paylaşımında bulunmalarına imkân vermesi demektir. Sosyal medya sizin kim olduğunuz ile ilgili ilgilenmez, önemli olan o alanda bulunmanızdır. Kullanıcılar da bu durumdan faydalanarak bazen gizlenerek gerçek kimliklerini sosyal ağdaki paylaşımlardan soyutlarken bazen de birilerini taklit ederek diğer kişileri kandırmaya çalışırlar. Bu durum "sahte hesap" kavramının çıkmasına neden olmuştur. İngilizce karşılığı genel olarak "fake account" olarak kullanılır.

Sahte hesap; insanların sosyal ağlarda kendi kimliklerinden farklı uydurma isim ve bilgilerle oluşturdukları hesaplardır. Sahte hesaplar kişinin sadece farklı bir isim kullanması ya da kendini gizlemesi değil, başka birini taklit etmesiyle de olur. Bu eğlence amacıyla olabilirken bazen de zarar vermek, kandırmak amaçlı olabilir (Kayaoğlu, 2013).

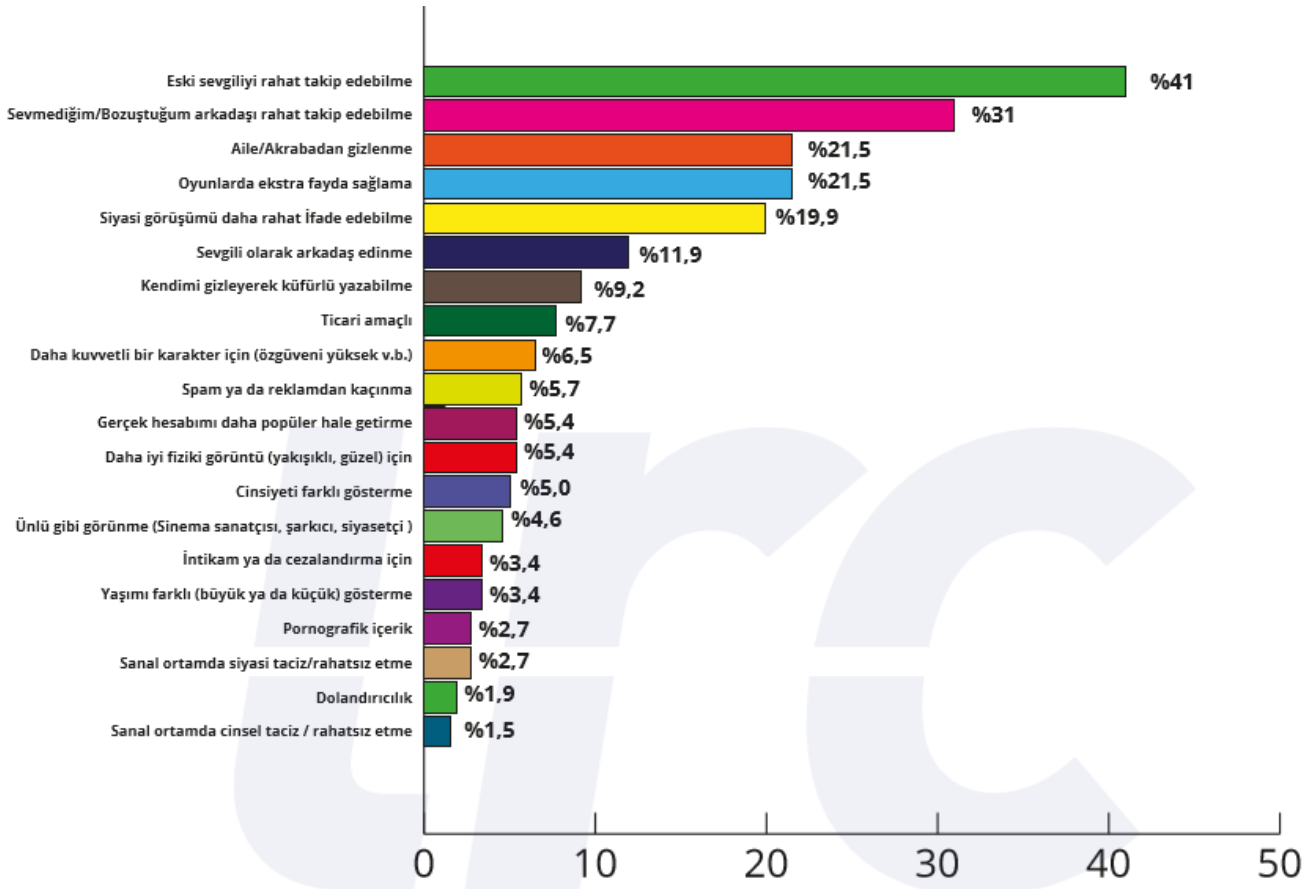
Bizim için önemli olan sahte hesaplardan gelen paylaşımlardır. Kendi kimliğini saklayan ya da başka birisini taklit ettiğini düşündüğümüz birinin verdiği bilgiye nasıl güvenebiliriz?

### **Sahte Hesap Açılmasının Nedenleri**

Sosyal ağlarda insanların sahte hesap ile iletişim kurma nedenleri çok çeşitli olsa da genellikle güven eksikliği, birilerinden korkma veya gizlenme, verilecek önemli haberin olası zararlarından korunma, erişilmek istenen bilgiye gizlenerek ulaşma, özel hayatta bir takım

heyecanlar yaşama, sansasyon yaparak kişi veya toplumları kargaşaya itme, fesat çıkarma gibi nedenlerden ötürü başvurduklarını söylemek mümkündür (Genel, 2016).

İnsan Toplum ve Teknoloji Derneği (İTTD) 2016 yılında “*Üniversite Öğrencilerinin Sosyal Ağlarda Sahte Hesap Kullanım Eğilimi Araştırma Projesi*” adlı çalışma yapmıştır. Bu çalışmaya göre sosyal medya kullanıcılarının neredeyse üçte birinin sahte hesabı olduğu sonucuna varılmıştır.



**Şekil 5:** Üniversite Öğrencilerinin Sosyal Ağlarda Sahte Hesap Kullanma Nedenleri

Nedenlere baktığımızda genel olarak sosyal medyada sahte hesapların özel amaçlar için kullanıldığı sonucu çıkmaktadır.

Sosyal medya sadece kişiler için değil kurum ve kuruluşlar için de önemli bir tanıtım ve etkileşim aracıdır. Sosyal medya kullanımı hem kolay hem ucuz, hem zaman ve mekân sıkıntısı olmadığı için ve daha fazla kişiye erişme imkânı verdiği için çoğunlukla firmalar tarafından tercih edilmektedir. Sosyal medyayı bir pazarlama alanı olarak kullanan firmalar kendileriyle ilgili

hesaplar açarak müşteri destek hizmetleri, tanıtım ve reklam çalışmaları gibi aktivitelerini gerçekleştiriyorlar. Ancak hesap açmak için herhangi bir önkoşul gerekmediğinden aynı firmaya ait birden fazla hesap olabiliyor. Artık sosyal ağ kullanımı o kadar arttı ki sırf küçük düşürmek, karalamak için rakip firmalar tarafından bile diğer firmalar adına sahte hesaplar açılabilir (Ahi, 2012). Bu durumda hem firmalar kendi adlarına açılmış olan sahte hesapları tespit edip engel olmakla sorumlu hem de bizler bilgi almak için girdiğimiz sosyal ağdaki hesapların gerçek bir hesap olup olmadığını anlayabilmekle yükümlüüz.

### **Sahte Hesap Örnekleri**

Sosyal medyadaki sahte hesaplarla başı derde girmiş olan pek çok kişi var. Bunlardan belki de en ilginç olan kişi Bilgi Teknolojileri ve İletişim Kurumu eski başkanı Tayfun Acarer. Acarer ismine kayıtlı Twitter’da sahte bir hesap vardı. BTK başkanı tam 1 seneye yakın o hesabı fark edememiş ve bu kişi kendini Acarer olarak tanıtarak insanlarla mesajlaşmış. Acarer *“Ben BTK başkanı olarak çıkartmakta zorlanıyorsam vatandaş ne yapacak? Bu ciddi bir sıkıntı”* diye belirtti. Twitter’ın bu konuyla ilgili çalışması bulunduğu bahseden Acarer, Twitter’ın arka planda çalışan bir uygulama ile sahte hesapları keşfettiğini ve sildiğini, ancak bu program sebebiyle durağan şekilde olan gerçek hesapların da silindiğini belirtti (HaberTurk, 2013). Medyaya yansıyan bir diğer örnek işadamı Ahmet Paksoy ile ilgili. Paksoy 10 Kasım 2014 tarihinde Ahmet Paksoy ismiyle açılan bir Facebook hesabından iş ve özel hayatıyla ilgili bazı ithamlar ve hakaretlerde bulunan sahte hesabı fark etti ve çevresindekileri hesabın kendisinin olmadığına dair uyardı ve sahte hesabın sahibi 20 dakika içerisinde siteden çıktı (Akdenizmanşet, 2014). Bu ve bunun gibi örnekler özellikle tanınmış kişilerin başına çok gelmektedir.



Şekil 6: Aydın Baruş Twitter Sahte Hesaplar

Yukardaki görselde görüldüğü üzere Twitter'da Bolu Valisi Aydın Baruş adına açılmış dört tane hesap olduğu ortaya çıktı, siz olsaydınız bunlardan hangisini takip ederiniz?



Şekil 7: Orhan Düzgün Sahte Twitter Hesabı

2015 yılında Kayseri Valisi Orhan Düzgün adına da sahte bir tweet hesabı açılıp okulların tatil edildiği bilgisi yayılmıştı. Kayseri Valisi durumu hemen fark edip hesabın kendisinin olmadığını belirtmiştir (Cnnturk, 2015).



**Şekil 8:** Ahmed Arif Facebook Hesabı

Yukardaki görseldeki bilgiye veren kişi Facebook'da Ahmed Arif adına bir sayfa açmış ve onun resimlerini kullanıyor. Ama gerçek Ahmed Arif olamayacağını biliyoruz çünkü şair ve gazeteci olan Ahmed Arif 1991 yılında vefat etti. Bu Facebook hesabını açan kişi büyük bir ihtimalle Ahmed Arif'i seven bir kişi olarak düşünülüyor ama gerçek kimliğini kimse bilmiyor buna rağmen binlerce de takipçisi mevcut. Bu kişi yukarda gördüğümüz görseli paylaşarak; Avusturya'daki Türk vatandaşlarının vatandaşlıktan çıkmak için konsolosluk önünde uzun kuyruk oluşturduğu bilgisini verdi ve hiçbir kaynak belirtmedi. Kendisini takip edenlerin büyük çoğunluğu bilgiye inanarak tartışmaya başladı. Ancak teyit.org sitesinin yaptığı inceleme ile resmin aslında Almanya'da olduğu ve kuyruğun da oy verme kuyruğu olduğunu açıklandı.



**Şekil 9:** Ahmed Arif Facebook Hesabı - teyit.org

Burada bu bilgiyi veren Facebook hesabı Ahmed Arif bu bilgiyi nerden almıştı? Kendisi gibi bir sahte hesaptan alıp inanmış ve paylaşmış da olabilir ya da sadece insanları çatıştırmak için de yapmış olabilir. Maalesef yanlış bilgi yaymak çok kolayken bilginin doğrulanması süreci uzun sürmektedir. Bu nedenle bir bilgiyi doğrulanmadan kesin şekilde inanmamak gerekir. Hele ki kim olduğunu bilmediğimiz hesapların verdiği bilgiler için kaynak istememiz kesinlikle gerekir.

Sahte hesapların firmaları taklit ederek onlara zarar verirken, yanlış ve eksik bilgilerle diğer insanları da yanıltıklarından bahsetmiştik. Firmalar adına açılan sahte hesaplar hakkında aslında nadir de olsa iyi örnekler bulunmaktadır. Örneğin bir genç, Sony marka eşyaların kullanıcılarına yönelik bir forum sitesi açmış ve bu site zamanla çok popüler hale gelmiş. Sony de bu durumu fark edip siteyi açan genci dolgun bir maaşla yönetici yaparak siteyi satın almış ve

resmi bir kullanıcı topluluğu haline getirmişler. Bu olay, marka adına açılan sahte hesapların her zaman kötü olmayabileceğinin kanıtıdır (Ahi, 2012).

Yukarda verilen örnekler birilerinin kendini gizlediği, başkası gibi davrandığı hesapların örnekleridir. Bir de insan olmayan sahte hesaplar var. Makinalar tarafından otomatik oluşturulan ve kodlanarak kendiliğinden takip etme, beğenme, paylaşma gibi aktiviteler gerçekleştiren robotik sahte hesaplar mevcut. Sosyal ağlarda topladıkları verilerle sahte kullanıcı profilleri oluşturan yazılım programları ile oluşan bu sahte hesaplara “bot hesap” denmektedir.

### **Bot Hesaplar**

İngilizce robot kelimesinin kısaltılması olan bot, bilişim dünyasında yaygın kullanılan bir terimdir (Ünver ve diğerleri, 2010). Aslında bot programlar insanların bilgisayarına gizlice yüklenerek bilgisayar üzerindeki bilgilere erişmek ve hassas bilgileri (hesap şifreleri, e-posta bilgileri gibi) çalmak için kullanılan zararlı yazılımlardır. Ancak sosyal ağlarda kullanılan bot hesap; dünyanın farklı yerlerinde oluşturulmuş, gerçek hesap görünümünde olan ancak bir sistem tarafından yönlendirilen sahte takipçi olarak kullanılır (wmaracı, 2017). Bot takipçi hesapları bazen bilgisayar yazılımları ile kodlarla oluşturulan sahte kişilerken bazen de veri hırsızlığı yardımı sayesinde oluşturulabilir. Örneğin; Twitter, Facebook, Youtube gibi ağlarda hazırlanan zararlı bir uygulama, hesabınızın başkalarını takip etmesini sağlayabilir. Bu durumda siz de farkında olmadan birer bot takipçiye dönüşebilirsiniz (wmaracı, 2017).

Peki, insanlar neden bot hesap takipçisi satın alır? Genellikle takipçi sayısı arttırmak için bot hesaplar satın alınır. Bunun en önemli nedeni popülerlik. Bot takipçiler sayesinde hesabın olduğundan daha güvenilir ve etkileşimi yüksek bir hesap olduğu imajı oluşturularak hesabın daha çok etkileşim elde etmesi ve içeriklerinin daha çok kişiye ulaşması mümkündür (wmaracı, 2017). Eğer bir tweet çok fazla beğenildiyse, Youtube’da bir video çok fazla izlendiyse popüler olma olasılığı da o kadar artar. Popüler olan konular da gündemi etkileyebilir. Eğer aynı anda aynı hashtag (#etiket) üzerinden aynı mesajlar paylaşırsa bir kamuoyu yaratılabilir.

Oxford İnternet Enstitüsü’nde bot araştırmacısı olarak çalışan Profesör Philip Howard bot hesapları internetteki tartışmaları yönlendirmek isteyen politikacıların da kullandığını belirtmektedir. Bot hesaplar, bir politikacıya desteğin olduğundan daha yüksek olduğu algısı oluşturabiliyor. Hatta bazen bot hesaplar bazı anahtar kelimeler gündeme geldiğinde kendiliğinden

diğer bot hesaplarla ve gerçek kullanıcılarla bir tartışma başlatabiliyor (Baerthlein, 2016). Donald Trump'ın seçildiği başkanlık seçimiyle ilgili yapılan bir araştırmada Trump'ı destekleyen pek çok bot hesap olduğu ve bu hesapların tweet attığı ortaya çıkmıştır. Yani kalbi ve düşünme yetisi bulunmayan robotlar sadece takip etmek ve beğenmek dışında tweet atarak bilgi de sağlayabiliyorlar (Dewey, 2016). Profesör Howard eskiden popüler olmak için kullanılan botların artık negatif mesajlar, yanlış bilgiler, şüphe ve hatta nefret dolu konuşmalar yapan canlılar olduğunu söylemektedir (Dewey, 2016). Teknolojinin gelişmesi ile bilginin giderek arttığı günümüzde artık bilgi sadece insanlar tarafından değil insan görünümü makinalar tarafından da verilmektedir.

“Bot” ve “activist” kelimelerinin birleşimiyle “botivist” terimi ortaya çıkmıştır. Virginia Üniversitesi'nde asistan profesör olan Saiph Savage, iyi bir iletişim sağlamak için botivist hesap kullanılabileceğini belirtiyor. Örneğin yolsuzluktan şikâyet eden vatandaşlar ile temasa geçerek yolsuzlukla mücadele için neler yapılabileceğini soran bir botivist hesap olabilir. Bu sayede sosyal medyada çok daha fazla insana ulaşılabilir, bir topluluk oluşturulabilir. Savage, botivist hesapları insanları cesaretlendirici hesaplar olarak görüyor. Ancak Savage botivistlerin gerçek insanmış gibi davranmamaları gerektiğini, internet ortamında kendilerini bir çeşit makineye adadığını fark eden insanların kandırılmış hissedeceklerini söylüyor (Baerthlein, 2016). Baerthlein'in yazısında belirttiğine göre Meksika ve Türkiye en çok bot hesabın bulunduğu iki ülke.

Bot hesaplar kimler tarafından üretiliyor? Bunları sağlayan pek çok firma ya da yazılım mühendisleri bulunmaktadır. Eğer böyle bir niyetiniz varsa internette basit bir arama yaparak pek çok siteye ulaşabilirsiniz. Örneğin; <https://crovu.co/> adresli bu firma Instagram, Facebook, Twitter, Youtube gibi farklı sosyal ağlarda takipçi satın almanızı sağlıyor ve bunun için paket hizmetler dahi veriyorlar.



Crovu'nun eşsiz paketleriyle Twitter Takipçi satın al. Hesabını popüler yapmak senin elinde!

<b>1000</b> Twitter Takipçi	<b>2500</b> Twitter Takipçi	<b>5000</b> Twitter Takipçi
<b>29<sup>99</sup></b> ₺	<b>55<sup>99</sup></b> ₺	<b>99<sup>99</sup></b> ₺
Yüksek Kaliteli Takipçi	Yüksek Kaliteli Takipçi	Yüksek Kaliteli Takipçi
Şifreniz Gerekmiyor!	Şifreniz Gerekmiyor!	Şifreniz Gerekmiyor!
Başkalarını Takip Etmeniz Gerekmiyor!	Başkalarını Takip Etmeniz Gerekmiyor!	Başkalarını Takip Etmeniz Gerekmiyor!
2 Saat içinde Hızlı Teslimat	2 Saat içinde Hızlı Teslimat	2 Saat içinde Hızlı Teslimat
7/24 Canlı Destek Email - Telefon	7/24 Canlı Destek Email - Telefon	7/24 Canlı Destek Email - Telefon
<b>Hemen Satın Al!</b>	<b>Hemen Satın Al!</b>	<b>Hemen Satın Al!</b>
<b>10000</b> Twitter Takipçi	<b>15000</b> Twitter Takipçi	<b>20000</b> Twitter Takipçi
<b>169<sup>99</sup></b> ₺	<b>229<sup>99</sup></b> ₺	<b>289<sup>99</sup></b> ₺
Yüksek Kaliteli Takipçi	Yüksek Kaliteli Takipçi	Yüksek Kaliteli Takipçi

**Şekil 10:** Twitter Takipçi Satın Alma

Görünen o ki bot hesaplar gün geçtikçe artıyor ve bu alanda rekabet yapan firmalar bile ortaya çıkmış durumda. Kimi araştırmacılar bot hesaplar için olumsuz düşünürken kimi araştırmacılar faydaları üzerinde duruyor. Doğru bilgiye erişmek istiyorsak iyi veya kötü niyetli olsun bir makine tarafından ortaya atılan bir bilginin doğruluğuna her zaman şüpheli yaklaşılması gerektiğini unutulmamalıdır. Bunun için en temel olarak da sanal ortamdaki hesapların sahte ya da bot olup olmadığını anlayabilmemiz gerekmektedir.


## Sahte Hesap Doğrulama Araçları

Sosyal mecralarda giderek daha büyük bir problem olan bilgiyi doğrulama sorununa yönelik çalışmalar yapılmaktadır. Bu çalışmalardan birinin sonucu olarak da “Verification Handbook” ortaya çıkmıştır. Bu kitabın öncelikli hedefi gazeteciler ve sivil toplum çalışanları olarak belirlense de aslında herkesin yararlanabileceği bir kaynaktır. Detaylı şekilde yazılmış yol gösterici olan Doğrulama El Kitabı’nın içinde bazı kaynak doğrulama araçlarına da yer verilmiştir. Bu araçlar şunlardır: AnyWho, AllAreaCodes, Facebook Graph Search, GeoSocial Footprint, Hoverme, Identify, Linkedin, Muck Rack, Numberway, Person Finder, Pipl.com, Rapportive, Spokeo, WebMii, WHOIS

Doğrulama El Kitabı’nın içinde olan bu araçların yanına daha pek çok araç da eklenebilir. Örneğin; Twitter’da sahte hesap takiplerini tespit eden <http://fakers.statuspeople.com/> ve <https://www.twitteraudit.com/> gibi ya da Instagram’da bot hesapları bulan <http://www.followercheck.co/> gibi. Bunlar gibi daha pek çok ücretli ve ücretsiz araçlar geliştirilmiş ve geliştirilmektedir. Önemli olan araçların sayılarının çok olması değil gerçekten faydalı olup olmadıklarıdır.

Eğer karşınıza çıkan bir hesabı herhangi bir doğrulama aracı olmadan değerlendirebilmek istiyorsanız bazı temel şeylere göz atarak fikir edinmeye çalışabilirsiniz. Örneğin:

- Hesabın sosyal ağ üzerindeki geçmişini kontrol edin: Ne kadar aktif? Ne hakkında konuşuyor, ne paylaşıyor?
- Bu hesap ne zamandan beri aktif? Uzun süredir var olan ve daha aktif bir hesabın diğer hesaplara göre daha güvenilir olduğu varsayılabilir.
- Hesapta belirgin biyografik bilgiler nelerdir? Konum bilgisi, iş bilgileri gibi
- Sosyal medya üzerinde kimlerle bağlantıda; arkadaşları ve takipçileri kimler?
- Kullandığı görselleri aratarak orijinal mi yoksa bir yerden mi alınmış kontrol edebilirsiniz.
- Diğer sosyal ağlar üzerinde aynı kullanıcı adı ile bir arama yapın ve diğer hesapları bulmayı deneyin. Örneğin Facebook hesabı olan kişinin bir de Twitter adresi olup olmadığına bakabilirsiniz. Ya da LinkedIn gibi ağları kontrol ederek iş geçmişini öğrenmeye çalışabilirsiniz. Google Plus, blog veya web sitesi üzerinde bir profili veya bağlı olduğu başka bir hesap var mı? Bağlı hesaplar bulursanız son konumu, aktivitesi, güvenilirliğine ilişkin hangi bilgiler gösterilmektedir?

Sosyal paylaşım sitelerinde hesapların doğrulanması üzerine bazı çalışmalar yapılmaktadır. Bunlardan son yıllarda en çok gördüğümüz uygulama ise “Onaylanmış Hesap” diğer adıyla “Mavi Tik”. İngilizce terimi “Verified Account” olarak bilinen mavi tik bize o hesapların gerçek sahipleri tarafından açıldığını ve yönetildiğini belirtir. Örneğin, ünlü birinin ya da bir işletmenin Youtube kanalında mavi tik rozetini görüyorsanız bu kanalın gerçekten ilgili kişi ya da işletmeye ait olduğunu bilebilirsiniz. Bu sayede aynı isimle açılmış diğer kişi ve kurum hesaplarının orijinal hesaplar olmadığını bilirsiniz. Bilgisayar farenizi mavi tik rozetinin üstüne tutarsanız “doğrulandı” ya da “doğrulanmış” yazısının çıktığını görebilirsiniz. Kısaca mavi onay rozeti bir hesabın orijinal olduğunu insanların bilmesini sağlar. 



Şekil 11: Turkcell'in Facebook'da Doğrulanmış Sayfası

Ancak bu doğrulanmış rozet herkese verilmemektedir. Tanınmış ve ünlü kişilere ya da markalara, firmalara verilen bir rozettir. Twitter yardım sayfasında hangi tür hesapların onaylanabileceğine bakarsanız şu yazısı görürsünüz: “Kamuoyunun ilgisini çekebileceği belirlenen bir hesap onaylanabilir. Genel olarak bu hesaplar müzik, oyunculuk, moda, hükümet, politika, din, gazetecilik, medya, spor, iş dünyası ve diğer temel ilgi alanlarına mensup kullanıcılar tarafından kullanılır”. Eğer fazla takipçisi olan bir internet fenomeniyseniz siz de başvurarak şansınızı deneyebilirsiniz.

Peki, nasıl başvurulur ve alınır. Örneğin, Twitter’da mavi tik rozeti alacaksanız bunun için Twitter’a istekte bulunarak bir form doldurmanız gerekmektedir. Sizden isteyecekleri bilgiler:

- Doğrulanmış e-posta adresi
- Doğrulanmış/Onaylanmış bir telefon numarası
- Doğum Tarihi
- Twitter’de biyografi bölümünün doldurulmuş olması
- Geçerli bir profil fotoğrafı
- Twitter hesabının tüm kullanıcılara açık olması
- Varsa kişisel blog ya da web sitesinin adresi

Bu bilgileri girerek başvuruda bulunmuş oluyorsunuz. Sizinle ilgili gerekli incelemeleri yaptıktan sonra eğer uygun görürlerse size onaylanmış hesap anlamına gelen mavi tik rozetini ekliyorlar. Diğer sosyal mecralarda da sistem aynı şekilde işliyor.

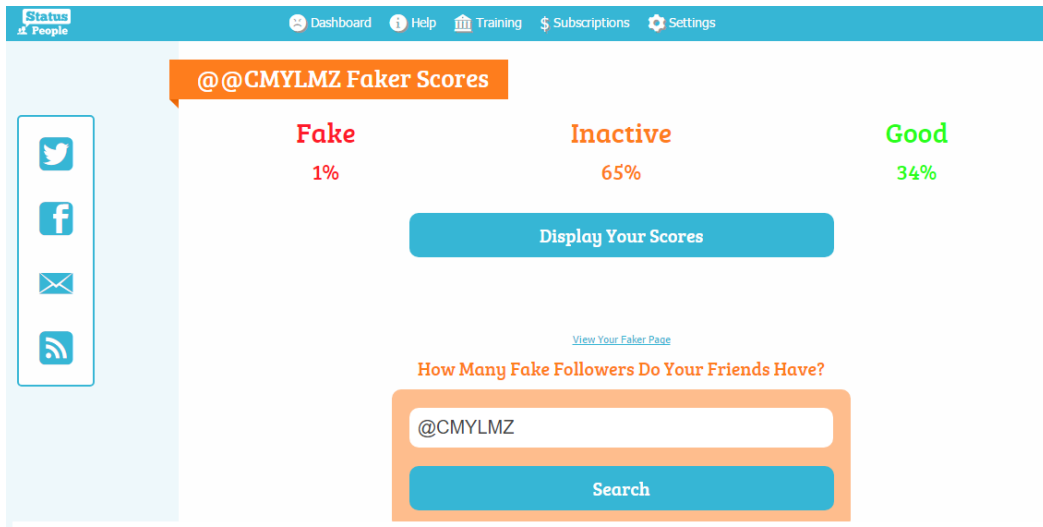
İlk onaylanmış hesap akımı 2009’da Twitter tarafından başlatıldı. İlk zamanlarda kullanıcılar mavi tik rozetine sahip olabilmek için Twitter’a herhangi bir başvuruda bulunamıyordu, Twitter düzenli aralıklarla hesapları onayladıklarını, en çok aranan kullanıcılara odaklanmış durumda olduklarını ve normal kullanıcıların hesaplarını onaylamadıklarını söylüyorlardı. Daha sonra Google+ ve Youtube Ağustos 2012’de onaylanmış hesap rozetini vermeye başlayan sosyal medya mecralar oldu. Facebook Mayıs 2013’te mavi tik rozeti vermeye başladı ve başvuru için kullanıcılara bir form doldurma imkânı tanıdı. Aralık 2014 itibarıyla Instagram da mavi tik rozeti veren mecralar arasına katıldı. Instagram da Twitter’a benzer şekilde mavi tik rozetini tanınmış kişilere, ünlülere ve dünyada bilinen markalara veriyor ve yine Twitter’a benzer şekilde doğrulanmış hesap talebinde bulunulmasını engelliyordu. Türkiye’de ilk Instagram mavi tik rozetini profiline ekleyen iki marka ise Turkcell ve Gnctrkcell oldu (Ünlü, 2015). Zamanla mavi tik için başvurular ile ilgili geliştirmeler yapılmış ve bu uygulama farklı alanlara da yayılmaya devam etmiştir. Mavi tik rozetinin gerek kişilerin güvenilirliği gerek marka imajı için itibar artırıcı özelliği göz önüne alındığında bunun güzel bir uygulama olduğunu söyleyebiliriz.

## BULGULAR VE DEĞERLENDİRME

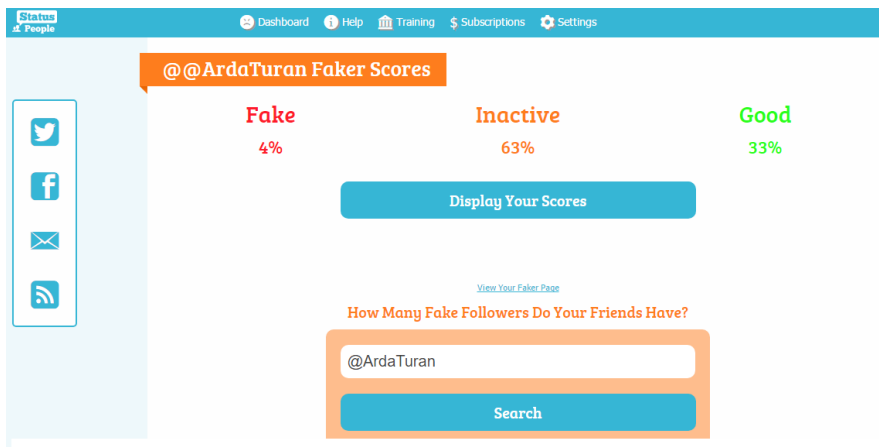
### Sahte Hesap Bulma Araçları Uygulama

Uygulama bölümünde bazen kendi hesaplarımı kullanarak bazen başka hesapları kullanarak Twitter, Facebook ve Instagram'la ilgili sahte hesap bulma araçlarını kullandım.

Twitter için hazırlanmış olan bir uygulama: <http://fakers.statuspeople.com/>. Bu uygulama Twitter'da sahte takipçi sayısını öğrenmeyi sağlıyor. Uygulamayı denemek için Cem Yılmaz ve Arda Turan'ın resmi Twitter hesaplarına bakıldı.



Şekil 12: Fakers.statuspeople Cem Yılmaz



Şekil 13: Fakers.statuspeople Arda Turan

Uygulama sonunda gelen sonuç sayfasında kişilerin takipçilerinin yüzde kaçının sahte olduğu bilgisini “fake” altında veriyor. Ancak bulunan sahte hesaplar genellikle bot hesaplar oluyor, bunun daha ötesinde pek bir şey yapıyor denemez. Bu uygulama daha çok Twitter’da bot takipçi satın alan kişileri ortaya çıkarmak için kullanılan bir uygulama. Örneğin; Erol Köse’nin Twitter hesabı üzerinden yapılan bir uygulamada fake oranı %41 çıktığı için sahte takipçi satın almakla suçlanmış ve bunun imajını zedelediği söylenmişti.

**StatusPeople Fake Followers, hesabını kullanmak üzere yetkilendirilsin mi?**

Beni hatırla - Şifreni mi unuttun?

**Bu uygulama şunları yapabilecek:**

- Zaman akışındaki Tweetleri okumak.
- Takip ettiğin kişileri görmek ve yeni kişiler takip etmek.
- Profilini güncellemek.
- Senin adına Tweet göndermek.

**Şunları yapamayacak:**

- Özel mesajlarına ulaşmak.
- E-posta adresini görmek.
- Twitter şifreni görmek.

  
StatusPeople Fake Followers  
Tarafından StatusPeople Ltd  
fakers.statuspeople.com  
Check your Twitter account for Fake Followers

**Şekil 14:** Fakers.statuspeople Twitter

Uygulamayı denerken karşıma çıkan sayfada bir şey dikkat çekiyor. Eğer uygulamaya izin verirsem yeni kişiler takip ederek benim adıma tweet gönderebileceği ile ilgili maddeler bulunmakta. Bu maddeler benim haberim olmadan beni bir bot hesaba çevirebileceği düşüncesi verdiği için uygulamayı güvenilir gözükmemektedir.

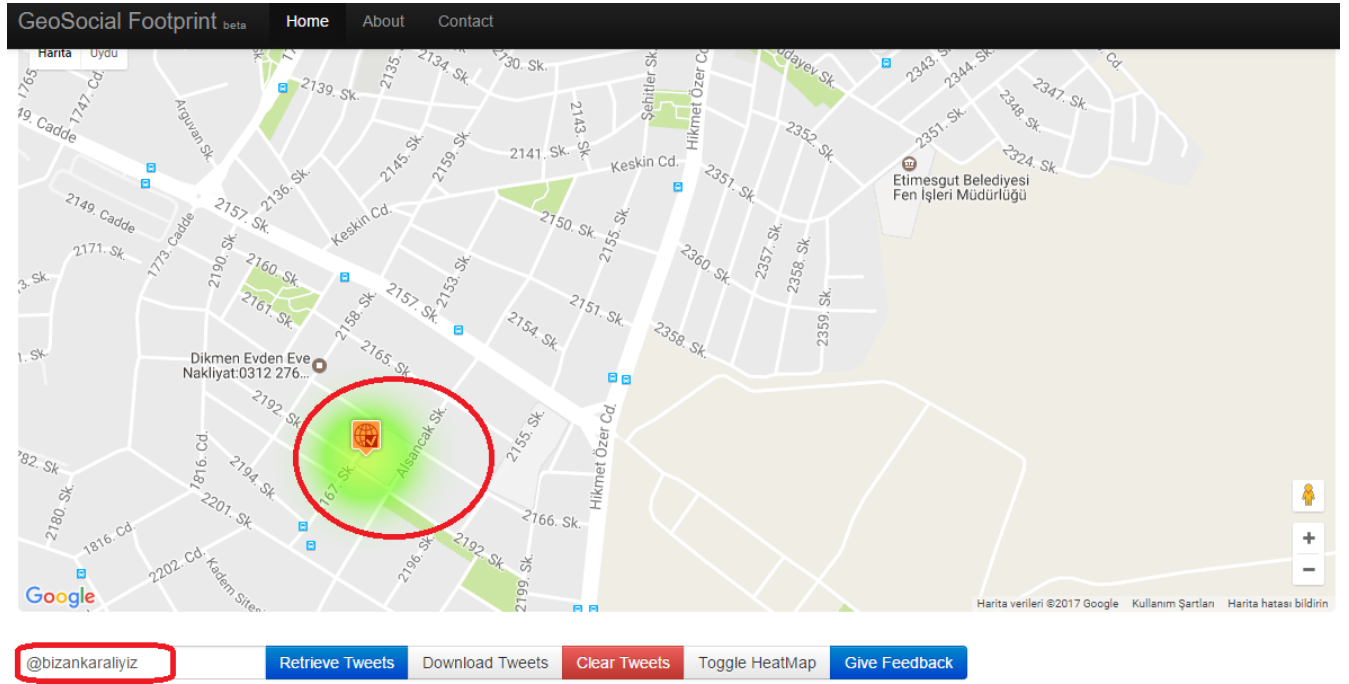
Twitter için bir diğer uygulama: <https://www.twitteraudit.com/>. Bu uygulama fakers.statuspeople.com ile aynı mantıkta çalışıyor, bir Twitter kullanıcı adını yazıp Audit’e tıklayarak aradığınız hesabın takipçilerinin yüzde kaçının sahte kaçının gerçek olduğunu size bildiriyor. Ben bu uygulama için NTV haberin resmi Twitter sayfası kullanıldı.



**Şekil 15:** Twitter Audit Report NTV Haber

Görüldüğü üzere NTV haber sitesinin sahte takipçileri gerçek takipçilerinden daha fazla çıktı. Ama bu uygulama hesapları değerlendirmek için nasıl bir mantık izledi? Diğer uygulama gibi sadece bot hesaplara mı odaklandı ya da başka algoritmaları mı var bilmek gerekli. Twitter Audit'in ücretsiz versiyonu ile sadece ne kadar gerçek ve sahte olduğunun sayılarını öğrenebilirsiniz. Eğer sahte olduğu düşünülen takipçileri engellemek ve düzenli olarak yeniden denetlemek isterseniz profesyonel versiyonunu kullanmanız gerekmektedir. Uygulamanın gösterdiği sahte olabilecek hesapları teyit etmek isterseniz gösterdiği hesapları tek tek kontrol ederek, kendiniz inceleyerek eleyebilirsiniz. NTV haber sitesi sahte hesap olarak gözüken hesapları listeleyerek kendilerine yorum yapan, bilgi veren hesapların bu listede olup olmadığını kontrol ederek kendilerini sahte hesaplardan gelecek yalan, yanlış bilgilere karşı koruyabilirler.

Twitter'la ilgili başka bir uygulama: <http://geosocialfootprint.com/>. Bu uygulama ile Twitter'da kullanıcı adını bildiğimiz birini aratarak konum bilgisi açık şekilde atılmış olan tweetlerden yola çıkarak kişinin yerini saptayabiliyoruz. Bunun için Twitter'da rastgele bulunan hesap ismi @bizankaraliyiz olan kişiyi denenerek konumu arandı.



Şekil 16: GeoSocial Footprint Arama Sayfası

Yukardaki görselde görüldüğü üzere bu hesabın sahibinin tweetlerinin çoğunu Ankara'da'ki bir konumdan attığı doğrulandı. Ancak konum bilgisini doğrulamak kişinin sahte veya gerçek olduğunun kesin bir kanıtı sayılmaz. Bu bilgi sadece doğrulama için yardımcı olabilecek bilgilerden biridir. Ayrıca bu bilgi güvenlik tehdidi de sayılabilir. Ben bu kişiyi hiç tanımayan biri olarak sokak numarasına kadar çevrimiçi bir uygulama sayesinde buldum. Kötü niyetli kişilerin kullanımına geçebileceği düşünüldüğünde sonuçları zararlı olabilecek bir uygulama. Her ne kadar işini yapsa da böyle bir uygulamaya herkesin kolaylıkla erişmesi bir sorundur. Bu yüzden sosyal ağlarda paylaşım yaparken daha dikkatli olmalıyız.

İsim, e-posta, telefon numarası ile arama yaptığınızda size aradığınız kişiyle ilgili sosyal ağlardaki sayfalarını gösteren <https://pipl.com/> adresli bir uygulama mevcut. Benim Facebook hesabımda hesap doğrulaması için telefon numaram kayıtlı ancak güvenlik ayarlarından telefon numaramı kapalı durumu getirdim yani benden başka kimsenin bu numaraya erişmesi mümkün değil. Bu sayfada kendi numaramla ilgili arama yaparsam sonuç getirip getirmeyeceğini kontrol ettim.

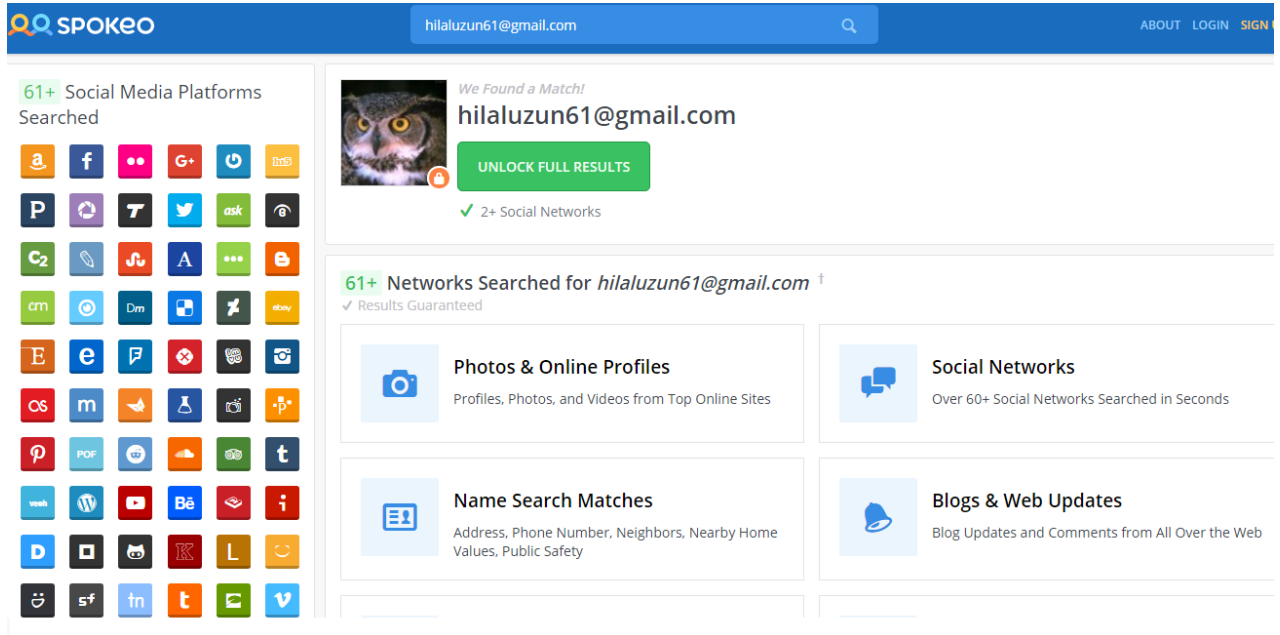




Şekil 17: Pipl Uygulaması Hesap Arama

Numaram kapalı durumda olsa bile yine de Facebook bağlantımı gösterdi. Bu şekilde eğer iletişime geçtiğiniz bir telefon numarası varsa ve bu numaraları sosyal mecralara kayıt ettilerse bulma şansınız var. Aynı şekilde mail adresimle arama yaptığımda da önceden açmış olduğum genç baykuş isimli blog sayfamı gösterdi. Ama e-posta ile kayıt olduğum Facebook, Instagram ve Twitter adreslerimi göstermedi sadece blog sayfasını getirdi. İsim olarak arama yaptığınızda sonuçlar çok fazla gelmektedir. Daraltma olarak da sadece yer ve yaş grupları (21-30, 31-40) seçeneklerini sunuyor. Bütün sosyal medya araçlarını da taradığı için isimle ilgili arama yaptığınızda içinden çıkılması zor bir hal almaktadır. Çözüm olarak daraltma seçeneklerini biraz daha fazla koyabilirler. Örneğin; konum yerlerine semtleri de ekleyebilirler, okul ve iş bilgilerini ekleyebilirler vs. Kısaca elinizde telefon numarası ve e-posta bilgisi varsa bu uygulamayı kullanmak mantıklı olabilir, diğer türlü isimle sonuca varmak zaman alıcıdır. Ayrıca elinizde kontrol etmek istediğiniz bir telefon numarası varsa deneyebileceğiniz çeşitli uygulamalar gene mevcut; <https://www.numberway.com/>, <http://www.kimbunumara.com/> gibi. Ama buralardan kişiye erişmek için numaranın sahibinin gizlilik ayarlarını açık bırakması gerekmektedir. Örneğin; kimbunumara.com'da benim telefon numaramda sadece isim bilgim açık, ilçe ve yasal sahiplik bilgileri görünmüyor.

Pipl.com ile aynı mantıkta çalışan bir diğer uygulama: <https://www.spokeo.com/>. Bu sitede de insanları isimleri, mail adresleri, telefon numaraları, adres bilgileri ile aratarak bulmaya çalışabilirsiniz. Ben burada kendi mail adresimi arattım.

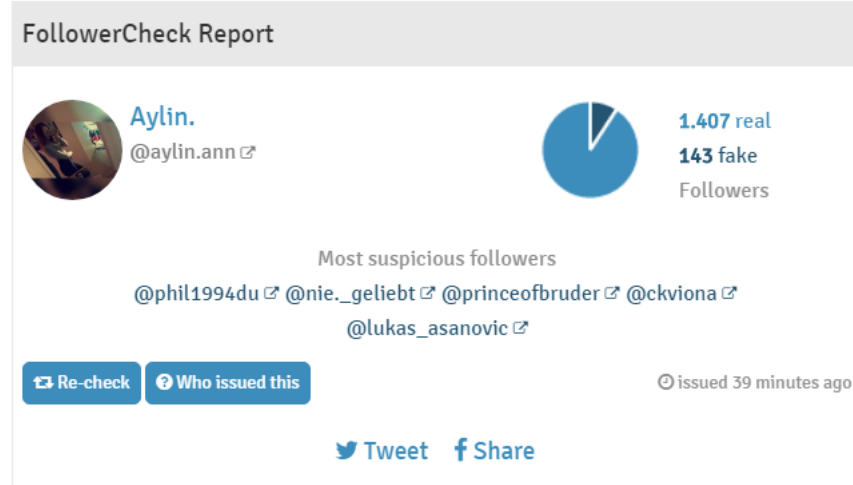


**Şekil 18:** Spokeo Uygulaması

Görseldeki tablonun sol kısmında görüldüğü gibi arama butonuna girdiğim e-posta adresini 61 sosyal medya platformunda arattı ve sonuç olarak iki sosyal ağ getirdi. Aslında benim üç tane sosyal ağda hesabım mevcut, bunlar; Facebook, Instagram ve Twitter. Hangi sosyal hesaplarımı bulduğunu göremedim çünkü üyelik istiyor. Ayrıntılı olarak bakmak için ücret ödemeniz gerekli. Ama getirdiği sonuç sayısına göre eksik bilgi verdi diyebiliriz. Ayrıca isimle arama yapıldığında sonuç getirmedi.

Bir diğer sosyal paylaşım ağı olan Instagram'daki takipçileri kontrol eden bir uygulama: <http://www.followercheck.co/>. Günümüzde markalar reklam yapabilmek için popüler kişileri kullanıyorlar. Bu kişilere ürünleri yollayarak tanıtım yapmalarını sağlıyor ve bu kişilerin takipçilerine erişmiş oluyorlar. Bu uygulamayı da reklam verme gibi düşüncemiz varsa, reklam vermeyi düşündüğünüz hesabın takipçilerini incelemek için kullanabilirsiniz. Binlerce takipçisi olan bir hesabın popüler görünmek için bot hesap satın alıp almadığını bu uygulama ile kontrol edebilirsiniz. Instagram'da rastgele karşıma çıkan bir hesap üzerinde deneme yaptım. Hesap yeni açılmış benziyor, 9 gönderisi bulunan hesabın 1550 takipçisi var. Bu takipçilerinin ne kadarın sahte ne kadarı gerçek, acaba bot hesap satın almış olabilir mi?

**FollowerCheck** Discover through FollowerCheck how many of your followers have a silicone heart



**Şekil 19:** Instagram FollowerCheck Uygulama

Sonuçta 1550 hesabın 143 tanesi sahte hesap çıktı. Sonuç raporunda sahte olduğundan şüphelenilen hesapların da linklerini vermektedir. Yani bu hesabın takipçilerinin çoğunun bot hesap olmadığı belli ancak hesabın kendisinin bot olup olmadığını ya da taklit olmadığını nasıl keşfedebiliriz? Bunun için bir çözüm sunmuyor.

Sahte olduğundan şüphelendiğiniz hesapların bakmanız gereken bir diğer özelliği de resimleridir. Sahte hesap sahipleri genellikle kendi resimlerini kullanmazlar. Kendileri gibi gösterebilecekleri uygun resimler bulup kullanırlar. Bunu tespit etmek için herhangi bir araca ihtiyacınız yok, Google görseller yardımıyla bir resmin nerelerde kullanıldığını kolayca bulabilirsiniz. Bunu yapmak için resmin url adresini kopyalayıp Google görseller bölümüne yapıştırıp aratmanız yeterli. Ya da bazen direk resme sağ tıklayınca “Google içinde resim ara” seçeneğini seçerek resmi aratabilirsiniz.

### Elif Taş on Twitter: "#takibetakup #takipedenitakipederim #GT ...



<https://twitter.com/.../708747626469060609> ▾ Bu sayfanın çevirisini yap

400 × 386 - Elif Taş · @eliftasss. Joined March 2016 .... Retweet 1; Likes 4; stubborn+++  
Elif Taş Komik Paylaşımlar kuzeyMavi. 12:12 PM - 12 Mar 2016. 0 replies 1 retweet ...

### yıldırım candaş (@halilkayaa1) | Twitter



<https://twitter.com/halilkayaa1>

73 × 73 - The latest Tweets from yıldırım candaş (@halilkayaa1). Olduğu kadar olmadığı  
kader.D. Yüreğ'in.

### Demek İsterdimki (@demekisterdimki) | Twitter



<https://twitter.com/demekisterdimki> - Bu sayfanın çevirisini yap

73 × 73 - The latest Tweets from Demek İsterdimki (@demekisterdimki)



Şekil 20: Google Görsellerde Resim Arama

Sosyal medyadaki bir hesabın profil resminde bulunan bir kadın fotoğrafı için bu uygulamayı denediğimizde aynı resim 3 farklı Twitter hesabında profil resmi olarak kullanılmış olduğu görülmektedir. Yani bu resmi kullanan hesapların sahte hesaplar olduklarından şüphe duyabilirsiniz.

## SONUÇ VE ÖNERİLER

Sahte hesap açmanın esas nedeni rahat hareket etmek denebilir. Yaptığımız, söylediğimiz, takip ettiğimiz, paylaştığımız hiçbir şeyden gerçek kimliğiniz etkilenmez. Ancak işin içinde insanlara saldırıda bulunmak, nefret söylemi, yanlış, yalan ve eksik bilgiler vererek insanları çatıştırmak gibi eylemler varsa sahte hesaplar hoş karşılanamaz. Kötü durumlara sebebiyet vermemesi, bilgi kirliliğine neden olamaması için de sahte hesapları tespit edebilmemiz lazım.

Sahte hesap bulmak üzerine geliştirilen araçların çoğu bot hesapları bulmak için programlanmış durumda. Arka plandaki yazılım bilgileri incelenerek bot hesapları bulmak 1-2

dakika süren bir eylem. Ancak bu konuda araçların eksik kaldığı yönler olmakta. Sosyal ağlarda uzun süre aktif kalmamış hesapları bu araçlar sahte hesap olarak algılayabiliyorlar. Bir hesabın durağan olması sahte olduğu anlamına gelmez ancak bu araçlar durağan hesapları da sahte olarak değerlendirebiliyorlar.

Bot hesapları bulmak için farklı sosyal ağlar için (Twitter, Facebook, Instagram vb.) farklı araçlar mevcut ancak başkasının yerine hesap açan birini keşfetmek çok zor. Eğer ünlü bir kişi ya da firma söz konusu ise mavi tik rozeti olan hesap dışındaki hesapların sahte olduklarını anlayabilirsiniz. Ancak tanınmış biri değilse başka birinin adına açılmış 2-3 tane hesaptan hangilerinin sahte hangisinin gerçek sahibi olduğunu anlamak zor. Bu yüzden birebir iletişime geçerek diğer sosyal alanlarda olup olmadığını kontrol ederek, paylaşımlarına bakarak vs. anlayabilmek bize düşen bir görevdir. Geliştirilen araçlar her ne kadar bot hesapları bulsa bile, bu araçlarla arkasındaki gerçek kişilerin bulunduğu sahte hesapları bulmaları şimdilik pek mümkün gözüküyor. Eğer iletişime geçtiğiniz bir hesap varsa bu kişinin kullanıcı adını aratarak adına kayıtlı başka hesaplar olup olmadığını bulmak, bulduğunuz hesaplardan hangisinin orijinal olduğunu anlamak için içeriği analiz etmek gibi işlemleri yine sizin yapmanız gerekmektedir. Tabii ki bazı kaynak doğrulama araçlarından yardım alabilirsiniz, örneğin; konum doğrulama araçları ya da kullandığı görselleri doğrulamak için çalıştırılan araçlar gibi. Çoğu araç e-posta, telefon, konum bilgisi gibi bilgileri kullanarak hesapları doğrulamaya çalışmaktadır. Ancak hesapların gizlilik ayarları sıkı bir şekilde yapıldığı, iletişim bilgilerini tam ve açık şekilde vermediği sürece bu araçları kullanmak çok zor olacaktır. Adınıza sahte hesap açan kişiyi bulmak için yapabileceğiniz en temel ve kesin çözüm IP adresini bulmak olacaktır. Bunu yapmak için hukuki yollara başvurmanız gerekmektedir.

Sonuç olarak bir hesabı bir sisteme koyduğunuzda size bunun sahte olup olmadığını kesin şekilde söyleyebilecek bir doğrulama aracı bulunmamaktadır. Bu yüzden sahte hesapları tespit etmek için geliştirilen çevrimiçi uygulamalar yeterli değildir görülmektedir.

Haberciliğin ana kurallarından sayılan 5N 1K (ne, neden, nerede, ne zaman, nasıl ve kim) sorularına cevap arayarak gidersek buna birden “kim tarafından” ya da “kaynak” ekleyerek bilginin sağlayıcısının da doğrulanması gerektiğini unutmamalıyız. Haberin içeriği kadar haberi verenin kimliği de önemli bir göstergedir. Kişinin mesleki ve toplumsal statüsü bilginin güvenilirliği konusunda her zaman yardımcı bir araçtır.

İnternet kullanımını arttıkça sosyal ağların kullanımını da artmaktadır. Artık çok küçük yaşlarda sosyal medya hesapları bulunan çocuklar mevcut. Bu yüzden ağaç yaş iken eğilir mantığı ile çocuklara küçük yaşta sahte hesapların ne olduğu ve nasıl anlaşılacağı üzerine bilgilendirmemiz lazım. Bu bilgilendirmeyi yapabileceğimiz en iyi yer de tabii ki eğitim yuvalarımız olan okullardır. Okullarda ortaöğretimden itibaren (sosyal/dijital) medya okuryazarlığı dersi zorunlu ders olarak okutulmalı, çocuklara sanal ortamdaki kişilerin kimliklerini doğrulayabilecek yöntemler göstermeliyiz.

Şüphe duyduğunuz bir hesap varsa bunun için birden fazla araç kullanarak doğrulamaya çalışın. Örneğin konum bilgisini kontrol edin, diğer sosyal ağlarda hesapları olup olmadığını kontrol edin, yüklediği resimlerin orijinal olup olmadığını kontrol edin. Adınıza açılan sahte hesap olup olmadığını düzenli aralıklarla kontrol edin ya da bunu kontrol ederek size bilgi verecek bir doğrulama aracından yardım alın.

Sahte hesap açmanın hukuki alanda da yaptırım eksikliği var sahte hesap açmakla ilgili güçlü bir cezai uygulama olması sahte ve bot hesapların önüne geçilmesini sağlayabilir.

Unutmayalım ki biz ne kadar doğrulama aracı geliştiresek de gelişen teknolojiyle birlikte bot hesaplar ve sahte hesap kullanan kişiler de kendini geliştirmektedir. Bu yüzden yapılan hiçbir araç tam anlamıyla mükemmel olamaz, her zaman geliştirilmeye ihtiyaç duyacaktır. Geliştirilen araçların güvenlik sınırlarını da iyi belirlemeliyiz. Bir hesabın gerçekliğini ispat edebilmek için de tüm bilgilerini başkalarına sunmak mantıklı bir eylem değildir.

## KAYNAKÇA

- Ahi, M. G. (2012). Şirketiniz adına sahte hesap açılırsa ne yapmalısınız? Erişim adresi: <https://gokhanahi.com/2012/12/09/sirketiniz-adina-sahte-hesap-acilirsane-yapmalisiniz/>
- Akdenizmanşet. (2014). Sahte hesap mağduru oldu. Erişim adresi: <http://www.akdenizmanset.com.tr/ozel-haber/sahte-hesap-magduru-oldu-h107877.html>
- Baerthlein, T. (2016). The rise of political bots on social media. Erişim adresi: <http://www.dw.com/en/the-rise-of-political-bots-on-social-media/a-19450562>
- Cnntürk. (2015). Sahte Twitter hesabı açarak Kayseri’de okulları tatil ettiler. Erişim adresi: <http://www.cnnturk.com/haber/turkiye/sahte-twitter-hesabi-acarak-kayseride-okullari-tatil-ettiler>
- Dewey, C. (2016). One in four debate tweets comes from a bot. Here’s how to spot them. Erişim adresi:

- [https://www.washingtonpost.com/news/the-intersect/wp/2016/10/19/one-in-four-debate-tweets-comes-from-a-bot-heres-how-to-spot-them/?utm\\_term=.440574d00ba2](https://www.washingtonpost.com/news/the-intersect/wp/2016/10/19/one-in-four-debate-tweets-comes-from-a-bot-heres-how-to-spot-them/?utm_term=.440574d00ba2)
- Genel, M. G. (2016). Sosyal medyada “kimlik bunalımı”: kripto hesaplar. *Yeni Medya Araştırmaları – 2*. Erişim adresi:  
[https://www.academia.edu/31111665/SOSYAL\\_MEDYADA\\_K%C4%B0ML%C4%B0K\\_BUNALIMI\\_Kripto\\_Hesaplar](https://www.academia.edu/31111665/SOSYAL_MEDYADA_K%C4%B0ML%C4%B0K_BUNALIMI_Kripto_Hesaplar)
- HaberTurk. (2013). BTK başkanı adına Twitter’da sahte hesap açıldı. Erişim adresi:  
<http://www.haberturk.com/video/ekonomi/izle/btk-baskani-adina-twitterda-sahte-hesap-acildi/95206>
- Kayaoğlu, H. S. (2013). Sahte hesapların analizi. Erişim adresi:  
<http://www.hasansabrikayaoglu.com/sahte-hesapların-analizi/>
- Twitter yardım merkezi. (?). Onaylanmış hesaplar hakkında SSS. Erişim adresi:  
<https://support.twitter.com/articles/20169568?lang=tr>
- Ünlü, I. (2015). Sosyal medyada “onaylanmış hesap” rüzgârı. Erişim adresi:  
<http://comtalks.com/2015/01/09/onaylanmishesap/>
- Üniversite öğrencilerinin sosyal ağlarda sahte hesap kullanım eğilimi araştırma projesi (2016). Erişim adresi: <http://docplayer.biz.tr/19310541-Universite-ogrencilerinin-sosyal-aglarda-sahte-hesap-kullanim-egilimi-arastirma-projesi.html>
- Ünver, M. ve diğerleri (2010). Köle bilgisayarlar ve köle bilgisayar ağları (zombi ve botnetler). *Bilim Teknoloji ve İletişim Kurumu*. Erişim adresi:  
<https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuv-enlik%2Fkba.pdf>
- Vural, Z. B. A. ve Bat, M. (2010). Yeni bir iletişim ortamı olarak sosyal medya: Ege üniversitesi iletişim fakültesine yönelik bir araştırma. *Journal of Yasar University*, 20(5), 3348-3382. Erişim adresi:  
[http://www.tasam.org/Files/Icerik/File/yeni\\_bir\\_iletisim\\_ortami\\_olarak\\_sosyal\\_medya\\_45f56af6-aa86-4840-a8db-21f4bb4ab1dd.pdf](http://www.tasam.org/Files/Icerik/File/yeni_bir_iletisim_ortami_olarak_sosyal_medya_45f56af6-aa86-4840-a8db-21f4bb4ab1dd.pdf)
- we are social (2017). Digital in 2017: Global overview. Erişim adresi:  
<https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview>
- wmaracı (2017). Bot takipçi nedir? Bot takipçi satışı ve bot takipçi kasma. Erişim adresi:  
<https://wmaraci.com/nedir/bot-takipci>