Hakemli - Süreli - Bilimsel Dergi
İNTERNET UYGULAMALARI ve YÖNETİMİ
Journal of
INTERNET APPLICATIONS and MANAGEMENT
2020 / 11(2)

QR Kod Güvenlik Farkındalığı Üzerine Ankara İlinde Bir Araştırma

A research on the QR code security awareness in Ankara

Mert Ogün BİLİR [1], mertogunbilir@gmail.com
Esma ERGÜNER ÖZKOÇ [2], eeozkoc@baskent.edu.tr

Received: 03.07.2020; **Accepted**: 04.12.2020

The QR codes (Quick Response Code), which were first used in the production area in 1994, have spread too many areas of life (marketing, advertising, object identification, product tracking, etc.) with the use of mobile devices as QR code scanners. Despite the increasing popularity of QR codes, (i) does not create any perceptions of vulnerabilities among users and on the contrary, arouses curiosity (ii) the amount of data in the QR code is considerable (sufficient to execute attacks), making the QR code a target for attacks. There are many security issues and risks such as malicious code execution, redirection to unsafe web addresses and violation of user privacy. In this study, attacks on QR code and countermeasures are presented. In this study, a social experiment was conducted in Ankara province in order to determine the level of awareness of individuals about possible security weaknesses of QR Codes in social life and the problems to be created. The young generation, who follows the technology and adapts quickly to new technologies, has been selected as the target audience and three different QR Codes (Plain, Instructional, and Illustrated) have been designed and posters have been prepared. Data obtained from an online questionnaire where scanners of QR Code posters are directed demonstrates that the motivation of users to scan QR Code posters that do not contain any information was mainly due to curiosity and it was concluded that the target audience had a lack of knowledge about potential threats and ways to protect themselves.

Keywords: *QR Codes, Security, Malware, Phishing Attacks, Mobile Device*

İlk olarak 1994 yılında üretim alanında kullanılmaya başlayan QR kodlar (Quick Response Code - Kare Kod) günümüzde mobil cihazların QR kod okuyucu olarak kullanımı ile hayatın birçok alanına (pazarlama, reklam, nesne tanımlama, ürün izleme vb.) yayılmıştır. Popülaritesi gün geçtikçe artan QR kodların bu denli sık kullanımına karşın, (i) kullanıcılar arasında herhangi bir güvenlik açığı algısı yaratmaması ve aksine merak uyandırması, (ii) QR koda kaydedilebilen veri miktarının azımsanmayacak kadar fazla (saldırı düzenlemek için yeterli) olması QR kodu saldırılara hedef haline getirmiştir. Zararlı kod çalıştırılması, güvenli olmayan web adreslerine yönlendirme, kullanıcıların gizliliğinin ihlal edilmesi gibi birçok güvenlik problemi ve riski mevcuttur. Bu çalışmada toplumsal yaşamda bireylerin QR kodların olası güvenlik zafiyetleri ve yaratacağı sorunlar hakkındaki farkındalık seviyelerinin tespit edilmesi üzerine Ankara ilinde bir sosyal deney yapılmıştır. Teknolojiyi takip eden ve yeni teknolojilere hızlı adapte olan genç nesil hedef kitle olarak seçilmiş, üç farklı QR kod (Sade, Talimatlı, Resimli) tasarlanarak afişler hazırlanmıştır. QR kod afişlerini taratanların yönlendirildiği çevrim içi anketten elde edilen veriler, kullanıcıların herhangi bir bilgi içermeyen QR kod afişlerini taratma motivasyonlarının esas olarak merak duygusundan ileri geldiğini göstermiş ve hedef kitlenin potansiyel tehditler ve kendilerini koruma yolları hakkında bilgi eksikliğine sahip oldukları sonucuna varılmıştır.

Anahtar Kelimeler: *QR Kod, Güvenlik, Kötü Amaçlı Yazılım, Kimlik Avı Saldırıları, Mobil Cihaz*

[1] Türk Elektronik Para A.Ş.-Turuncu Holding, İş Geliştirme Uzman Yardımcısı
[2] Başkent Üniversitesi, Ticari Bilimler Fakültesi –Yönetim Bilişim Sistemleri Bölümü (Sorumlu Yazar)

1. GİRİŞ

QR Kod (Quick Response), beyaz zemin üzerine siyah şekil ve motiflerden düzenlenmiş kare biçiminde bir barkoddur. Bir boyutlu geleneksel barkodlara göre, iki boyutlu karekodlar daha fazla bilgi aktarabilir ve depolayabilirler. 1994 yılında Denso firması tarafından otomobil endüstrisinde kullanılmak için geliştirilen QR kodu, kolay üretilişi ve dağıtımı, veri kapasitesi ve hızlı okunabilirliği nedeniyle popüler olmuştur.

QR kodlar günümüzde sıklıkla kullanıcıları daha fazla bilgi veya hizmet sağlayabilecek ilgi alanlarına ulaşmasını sağlayan web sitelerine yönlendirmek için kullanılmaktadır. Bunun yanı sıra birçok farklı uygulamada QR kodlar kullanılmaktadır. Bunlardan, otomatik plaka tanıma sisteminde (Moharil vd, 2012:5108), plakadaki sayı ve harflerin okunmasında karşılaşılan hatalara karşı plakalara QR kod eklenmesi önerilerek görüntü işlemedeki sorunlar giderilmektedir. Diğer bir uygulamada ise sektörlere göre değişen iş ekipmanlarının güvenliğini sağlamak, iş kazalarının sayısını azaltmak ve sürdürülebilir güvenlik önemlerini sağlamak için; asma iskele, yük asansörü, vinç vb. makinalara QR Kodlar yerleştirilerek, çalışanlara ve makinalara ait bilgilere kolay ulaşım ve kullanım kolaylığı sağlanmaktadır (Elçi, 2014:29-40). Pazarlama endüstrisinde ise QR Kodlar reklamcılığın tamamlayıcı bir yolu olarak kullanılmaktadır. Bir reklam, müşteriyi ürünle ilgili ek bilgilerin bulunduğu web sayfasına götürebilir. Örneğin, zincir süpermarket Tesco, çevrimiçi alışverişi artırmak ve Güney Kore pazarına daha fazla nüfuz etmek için QR kodları kullanmıştır. Bazı şirketler, QR Kod aracılığıyla, "tek tık" ile ödeme kabul etmektedirler. Müşteri ürünü satın almak için tanıtım posterinde bulunan QR kodu mobil telefonuna okutarak ödeme sayfasına veya şirketin web sayfasına yönlendirilmektedir. En büyük ödeme şirketlerinden olan Paypal, bu ödeme yöntemini bazı ülkelerde kullanmaya başlamıştır (Kapsalis, 2013:8). Görme engelliler için nesne tanımlama (Al-Khalifa, 2008) ise QR kodun kullanıldığı bir diğer alandır.

Günlük hayatta çok çeşitli alanda QR Kod kullanımı, birçok avantajının bulunmasına rağmen, güvenlik problemlerini de yanında getirmektedir. Bunun en büyük sebebi ise kodların insan tarafından çıplak gözle okunamamasıdır. QR Kod okumak için insanlar özel bir cihaz veya akıllı telefonlarını kullanmaktadır. QR Kod ile kullanıcılar kolayca bir kimlik avı web sitesi (phishing) veya bir kötü amaçlı yazılım dağıtıcı gibi kötü amaçlı bir web sitesine yönlendirilebilir. Bunun nedeni, kullanıcıların QR Kodda kodlanan bilgileri taramadan önce bilmemeleridir. Örneğin; stada küfür içeren pankart sokmanın yasak olduğu futbol müsabakalarında, Karşıyaka taraftarlarının Göztepe derbisinde küfür içeren bir URL'e yönlendiren QR Kod pankartı, polis aramasını kolaylıkla geçmiştir (Top, 2012) Bunlara ek olarak saldırganlar QR kodun okutulduğu cihazda kaydedilmiş özel verilere ulaşılabilir, kaydedebilir ve değişiklik yapabilir. Bu gibi farklı sebeplerle, saldırganlar çeşitli saldırı türleri için QR Kodları kullanmaktadır. Akıllı telefonların güvenlik düzeyinin arttırılması, kullanıcının mahremiyetinin korunması ve farkındalığının arttırılması amacı ile önlem alınması gerekmektedir.

Bir QR kodun içerebileceği en fazla binary veri miktarı 2.953 byte iken bu zamana kadar geliştirilmiş en küçük, kötü niyetli yazılım (crash. Pentium Trojan) 4 byte, SQL Slammer solucanı 376 byte'tır (Kieseberg vd., 2010: 430). Bu durumda bir QR kod, saldırı yapmak isteyen kötü niyetli kişiler için teknik açıdan yeteri kadar cezbedicidir. Şu ana kadar henüz

taratıldığında tüm sistemi yok edecek bir QR kod geliştirilmemiş olması, QR kodun potansiyel bir tehdit olduğu gerçeğini değiştirmemektedir.

QR Kod ile düzenlenebilecek çok sayıda saldırının varlığına rağmen QR Kodların bireyler için bir saldırı aracı olarak görülmemesi, risk algısının ve farkındalığın düşük olduğunu gösteren çalışmalar mevcuttur. Vidas ve diğ. (2013:52-69) amacı, QR Kodların kimlik avı saldırı vektörü olarak oluşturduğu tehdidi ölçmek ve QR kod etkileşiminin güvenliğini artırmanın yollarını belirlemek olan çalışmalarını 2012 yılında gerçekleştirmişlerdir. Çalışma iki farklı deneyi içermektedir; (1) QRishing deneyi: Bu deneyde, Carnegie Mellon üniversite kampüsü ve Pittsburgh şehri kamusal alanlarına 4 farklı el ilanı 4 hafta boyunca asılı kalmıştır. Kullanıcı QR kodu tarattığında çevrim içi anketin bulunduğu web sayfasına yönlendirilmiştir. (2) Gözetim deneyi: QR kod ile kullanıcı etkileşiminin kamera ile gözlenerek QR Kodu tarayan ancak ilgili web sitesini ziyaret etmemeyi seçen kullanıcıların oranını gözlemlemek için yapılmıştır. Çalışmada anketin bulunduğu web sayfası 225 kişi tarafından ziyaret edilmiş, anket 122 kişi tarafından doldurulmuştur. Anket sonuçları merakın QR kodları taramak için en büyük motive edici faktör olduğunu, gözetim deneyi ise, bir QR kodunu tarayanların %85'inin daha sonra ilişkili URL'yi ziyaret ettiğini göstermektedir.

Yin ve diğ.(2013) , akıllı telefonlarla QR kodları taramanın algılanan güvenlik riskleri üzerine yaptıkları çalışmada akıllı telefon kullanıcılarının QR kodu tarattıklarında kötü amaçlı bir web adresine yönlendirilirken aldıkları uyarı mesajına verdikleri tepkiyi (görmezden gelip ilerleme veya yönlendirmeyi iptal etme) araştırmıştır. Çevrim içi bir anket sitesi üzerinden yapılan çalışmaya 182 lisans ve yüksek lisans öğrencisi gönüllü olarak katılım sağlamıştır. Çalışmada cinsiyetin, coğrafi konumun (U.S., Macau) ve QR kodları önceden tarama deneyiminin, uyarı mesajının yok sayılması üzerinde önemli bir etkisinin olmadığı fakat bilgisayar ve teknolojide daha fazla deneyime sahip olan kullanıcıların, uyarı mesajlarını görmezden gelmelerinin daha muhtemel olduğu sonucuna varılmıştır.

Kapsalis, (2013:8) ise QR kodlar ile ilgili güvenlik konularında kullanıcıların güvenlik bilinci düzeyini belirlemeye yönelik ampirik bir çalışmayı Viyana, Helsinki, Atina ve Paris şehirlerinde yapılmıştır. Farklı konumlara yerleştirilen 3 farklı çeşit QR kod etiketleri taratıldığında (273 kişi), yönlendirilen çevrim içi anket 83 kişi tarafından doldurulmuştur. Anket cevapları kullanıcıların esas olarak merak duygularından motive olduklarını, potansiyel tehditler ve kendilerini koruma yolları hakkında ciddi bilgi eksikliğine sahip olduklarını göstermektedir. QR kodların Japonya'da, Avrupa'dan çok daha popüler olması sebebi ile Tokyo'da da yapılmak istenmiş fakat, Ulusal Enformatik Enstitüsü Etik Bölümünden istenilen gereklilikler yerine getirilemediği için anket yapılamamıştır.

Ülkemizde ise 2016 yılında, Göksel ve Başaran tarafından "QR-Code'daki olta bir farkındalık deneyi ve QR Kodların sosyal mühendislik saldırılarında kullanılması" sosyal deneyi yapılmıştır (Göksel & Başaran, 2016). Hazırlanan zararsız QR Kod afişleri Türkiye'nin çeşitli illerinde, üniversite ve sokaklarda 3 ay süresince asılı kalmıştır. Kullanıcılar tarafından taratılan QR Kodlar, "Oltalandınız! Ama paniklemeyin, Burada kötü niyetli kimse yok." Mesajını içeren bir web sayfasına yönlendirilmiş ve trafik izlenmiştir. Deneyde Ankara 3854 kişi, İstanbul 5101 ve Kıbrıs 72 kişi olmak üzere toplam kurban sayısı 9027 kişidir.

Özellikle İnternet kullanımının artması ve QR Kod okuyucuların akıllı telefon kameralarına entegre çalışması ile birlikte QR Kod kullanımı daha yaygın hale gelmiştir. Juniper Research

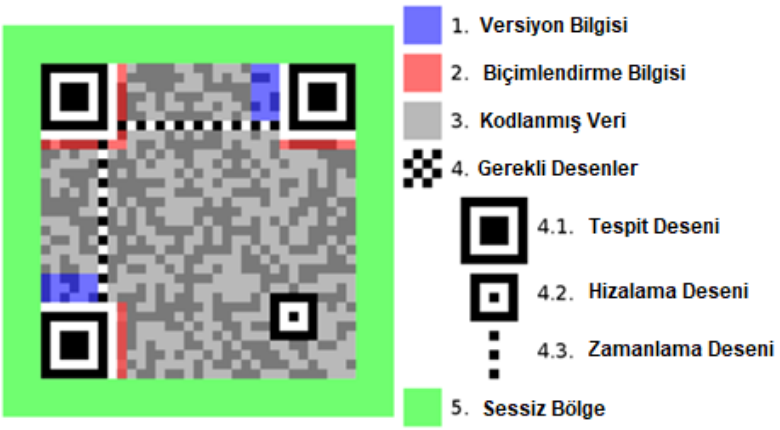
tarafından yapılan çalışmada, QR Kod kullanımının 2022'de 5,3 milyar seviyesine ulaşması, 1 milyar mobil cihazın ise QR Kodlara erişeceği tahmin edilmektedir (Juniper Research, 2020). Çalışmamızda, QR Kodların günlük hayatımıza entegre olduğu bugünlerde, akıllı telefon kullanan, teknoloji okur-yazar genç neslin QR Kodları taratma motivasyonları ve QR Kodlardan kaynaklanabilecek güvenlik zafiyetleri hakkında farkındalık düzeyi araştırılmıştır. Bu sebeple gerçeğe çok yakın şekilde QR Kod saldırı senaryosu tasarlanarak kişilere kaynağını ve amacını bilmediği halde tarattığı QR Kodların yönlendirdiği bir çevrim içi anket uygulanmıştır.

Çalışmanın ikinci bölümünde QR kodun yapısı, QR kod ile düzenlenebilecek saldırılar ve bu saldırılara karşı alınabilecek güvenlik önlemleri incelenmiştir. Üçüncü bölümde ise yapılan ampirik çalışmanın araştırma yöntemi, analiz ve bulgulara yer verilmiş, sonuç ve değerlendirme ile de çalışma sonlandırılmıştır.

2. QR KOD SALDIRILAR VE ÖNLEMLER

2.1. QR Kod Yapısı

Kırk farklı versiyonu bulunan QR Kodun, yaygın olarak kullanılan QR kod yapısı, Şekil 1'de gösterildiği gibi 5 temel alandan oluşur.



Şekil 1. QR Kod yapısı Kaynak: Polat 2014: 14-17.

1.*Versiyon Bilgisi:* QR Kodun sürümünü tanımlar. Her bir kodun veri depolama kapasitesi farklıdır. Depoladıkları veri arttıkça sürümleri de artmaktadır. Ek olarak kodların hata düzeltme seviyeleri de farklıdır.

2. *Biçimleme Bilgisi:* Biçimleme Bilgisi bölümü, ayırıcıların yanındaki 15 bitten oluşur ve QR Kodun hata düzeltme seviyesi ve seçilen maskeleme modeli hakkında bilgiyi içerir.

3. *Kodlanmış Veri:* Veri bu alanda depolanır. Veri, "0" ve "1" binary numaralarının siyah ve beyaz hücrelere çevrilmesiyle saklanmaktadır.

4. *Gerekli Desenler:* QR kodun üzerinde bulunan tespit, hizalama ve zamanlama desenidir.

4.1. Tespit Deseni: QR Kodun tüm köşelerinde, sadece sağ alt köşesi hariç olmak üzere üç aynı kareden oluşur. Bu kısım, okuyucu yazılımın QR kodunu tanımasını ve doğru yönlendirmesini sağlamaktadır. Bir piksel genişliğe sahip beyaz **Ayırıcılar (Seperators)** ile çevrelenerek tanınması ve gerçek verilerden ayrıt edilmesi kolaylaştırılmıştır. Bu şekillerde yapılan herhangi bir değişiklik kod çözücülerin kodu okumasını engelleyebilir.

4.2. Hizalama Deseni: Bu desen, QR okuyucunun kod büküldüğünde veya kavislendiğinde bozulmamasını ve düzeltmesini sağlar.

4.3. Zamanlama Deseni: Zamanlama deseninde bulunan alternatif siyah ve beyaz modüller, yazılımın tek bir modülün genişliğini belirlemesini sağlamaktadır. Sembol bozulduğunda veya hücre aralığı için bir hata olduğunda veri hücresinin merkezi koordinatını düzeltmek için hem dikey hem de yatay yönde düzenlenmiştir (Wane & Jamankar, 2013:176).

5. *Sessiz Bölge:* QR kodun çevresindeki verinin olmadığı boş alandır. Bu alana hiçbir şey yazılmaz ve basılamaz. En az 4 modül (her nokta 1 modüldür) genişliğinde olmalıdır. Bu boş alan sayesinde kod, hatasız bir biçimde okunmaktadır (Polat 2014: 14-17).

QR Kodda saklanabilecek veri miktarı, moduna, versiyonuna ve hata düzelme seviyesine göre değişiklik göstermektedir(Kieseberg vd., 2010: 430). Hata düzeltme seviyesi ise; Düşük (%7), Orta (%15), Kalite (%25), Yüksek (%30) şeklindedir [13].

QR Koda kodlanabilen veri, dört standardize edilmiş moddan birinde görülebilmektedir:

- Sayısal: En fazla 7.089 karakter (0,1,2,3,4,5,6,7,8,9)
- Alfa sayısal: En fazla 4.296 karakter (0-9, A-Z [yalnızca büyük harf], boşluk, $,%, *, +, -,., /, :)
- İkili / Bayt: En fazla 2.953 karakter (8-bit bayt)
- Kanji: En fazla 1.871 karakter

2.2. Saldırılar ve Önlemler

QR kodlar, hem insan etkileşimine hem de otomatik sistemlere saldırmak için kullanılabilir. Çalışmanın bu bölümünde düzenlenebilecek saldırılar ve bu saldırılara karşı alınabilecek önlemlere yer verilmiştir.

2.2.1. Saldırılar

SQL ve Komut Enjeksiyonu, otomatik sistemlere kolaylıkla, bilgisayar korsanları tarafından enjekte edilebilir. QR kod çözme yazılımının, bir veritabanına bağlandığı ve arka veritabanında bir sorgu yürütmek için QR kod bilgilerinin kullanıldığı bir senaryo olduğunu düşünelim. Böyle bir senaryoda, eğer QR kodu "1' OR '1'='1" gibi bir sorgu içeriyorsa (tırnak işaretleri olmadan), okuyucu kimliği doğrulanmış bir kaynaktan gelip gelmediğini doğrulamaksızın, okuyucu sorguyu çalıştırabilir ve bu bilgilerin başka türlü yetkili bir kullanıcı için tasarlanan potansiyel bir bilgisayar korsanına gösterilmesine yol açabilir. Bununla birlikte, QR kodları henüz veritabanı sorgulamaları sağlamak için kullanılmamıştır,

ancak yine de gelecekte QR kodları bu tür sistemlere saldırmak için kullanılabilir. Google, Google hesabına girişler için QR kodunu kullanma denemeleri yapılmıştır (Sharma, 2012).

Komut enjeksiyonu yönteminde ise saldırgan, sayfadaki içeriği değiştiren bir HTML kodu enjekte edebilir. Kullanıcı değiştirilen sayfayı ne zaman ziyaret ederse, web tarayıcı kodu yorumlar ve bu da kullanıcının QR kod okuttuğu cihazında (çoğunlukla akıllı telefon veya tablet) kötü amaçlı komutların yürütülmesine neden olur (Ahuja,2012: 38-78). Başka bir ifade ile QR koddan gelen giriş komut satırı parametresi olarak kullanıldığı bir durumdur. Böyle bir durumda, bir saldırgan QR kodu değiştirerek ve böylece sistemde rastgele komutlar çalıştırarak bu durumdan kolayca yararlanabilir. Bu şekilde bir saldırgan rootkit, spywares, Servis Engelleme (DoS) saldırısı başlatabilir veya uzaktaki bir bilgisayara bağlanabilir ve oradan sistemin kaynaklarına erişebilir (Sharma, 2012) .

Okuyucu yazılımının bilgisayarlarda veya akıllı telefonlarda farklı uygulamaları, komut enjeksiyonunun temizlenmemesi durumunda, komut enjeksiyonu veya geleneksel arabellek aşımı (buffer overflows) yoluyla saldırıya uğrayabilir. Saldırgan, kullanıcının iletişim bilgileri veya e-posta, SMS gibi iletişim içeriği de dahil olmak üzere tüm akıllı telefon üzerinde kontrol sahibi olabilir (Vidas vd., 2013:52-69) .

Sosyal mühendislik, yetkisiz olarak insanların gizli bilgilerine ulaşabilmek için manipüle etme sanatıdır. Bilgileri çalmak veya birinin erişmeye yetkili olmadığı bir sisteme zorla giriş yapmak için kullanılır. Sosyal mühendislikte en popüler uygulamalardan biri Kimlik Avı Saldırılarıdır (Phishing). Kimlik Avı, kullanıcıları, kullanıcı adları ve şifreler veya kredi kartı bilgileri gibi hassas kişisel bilgileri çalmayı amaçlayan yasal olan web sitelerini maskeleyerek sahte web sitelerine yönlendirme uygulamasıdır. Kimlik avı saldırılarındaki ana uygulamalardan biri, sahte web sitelerine veya kötü amaçlı yazılım içeren web sitelerine bağlantılar içeren kimlik avı e-postaları ve QR Kodlardır. QR kodun, bu saldırıda kolaylıkla kullanılabilmesinin ana nedeni kodun insan tarafından okunamamasıdır. Kullanıcı QR kodu okuyucu ile okuttuğunda ancak hangi URL'e yönlendirildiğini görebilmektedir. Sahte web sitelerine yönlendirdikten sonra, kullanıcı farkında olmaksızın bilgilerini girdiği zaman, kullanıcıya ait gizli bilgiler (kullanıcı adı ve şifre, hatta kredi kartı bilgileri gibi) dolandırıcıların eline geçmiş olmaktadır (Kapsalis, 2013:8) .

QR Kodlar, reklamlarda, hedef kitleyi özel tekliflere veya belirli ürünler hakkında ek bilgilere yönlendirmek için kullanılmaktadır. Saldırgan, QR kodlarının yerini alabilir ve kullanıcı taradığında, bilmeden sahte bir sayfaya yönlendirilebilir (Sharma, 2012). Saldırgan, kod okunduğunda kötü amaçlı yazılımın (Malware) otomatik olarak indirileceği bir sayfaya yönlendirilecek şekilde QR kodunda bir URL kodlayabilir. Saldırgan, bu şekilde virüs, casus yazılım, Truva atı veya kullanıcıya ve sisteme büyük zararlar veren solucanlar içeren yazılımın yayılımını gerçekleştirebilir. Eylül-Ekim 2011'de, Kaspersky Labs, bir web sitesinde bulunan mobil uygulamalar için QR kodlarda kısa mesaj gönderebilen "Truva atı" tespit etmiştir (örneğin, Jimm ve Opera Mini) (Wane & Jamankar, 2013:176).

Tarayıcı tabanlı saldırıları ve siteler arası komut dosyası çalıştırma saldırılarını (XSS/Cross Site Scripting) yürütmek için bir QR kodu kullanılabilir. Bir QR kodu şifreli URL içerebilir. Şifreli URL'nin tarayıcı da bir uyarı mesajı içerdiği senaryoda, kullanıcı URL'ye eriştiğinde, uyarı mesajı içindeki zararlı yazılım çalıştırılarak kullanıcının web tarayıcısı da dâhil kullandığı cihaza zarar verebilecektir.

Ayrıca, QR kod ile Dolandırıcılık/sahtekarlık (Fraud) amaçlı otomasyonlu sistemde değişiklikler yapılabilmektedir. Örneğin sistemi kandırarak, daha pahalı B ürününün kodunu ucuz bir A ürününün kodu ile değiştirip okuyucudan geçirmek için kullanılabilir (Kieseberg vd., 2010: 430). Sosyal medya hesabında çıkan sahte banka reklamlarında, linke tıklayıp çekilişe katılma hakkı kazanın, linkten mobil şubeye giriş yaparsanız ikramiye veya ödül kazanacaksınız gibi söylemlerle kullanıcılar kandırılabilmektedir. Kullanıcı linke tıkladıktan sonra dolandırıcı, kullanıcının girdiği bilgiler ile bankada işlem yapabilmektedir. Banka, kullanıcıya güvenlik için bir şifre göndermiş olsa da, kullanıcı o şifreyi de sahte web sitesine girdikten sonra (şifre kötü niyetli kişilerin eline geçerken) sadece hata mesajı almaktadır. Ancak kötü niyetli kişiler kişisel bilgi ve şifreye ulaştığı için, o şifre ile QR kodunu ele geçirip istediği ATM'den kullanıcı kartı olmadan işlem yapabilmektedir. Saldırgan bu yöntemler sadece cep telefonundaki QR kodu okutularak, banka hesapları boşaltılabilir, transferler yapabilir veya kullanıcı adına kredi çekebilir (Koygun, 2018). Ülkemizde bu yöntem ile para çekmeye çalışan bir kişi siber suçlar ile mücadele şube müdürlüğü tarafından yakalanmıştır (DHA, 2017). Öte yandan Çin Halk Cumhuriyeti Merkez Bankası, QR-kod ödeme sistemi Çin içerisinde kara para aklamak ve dolandırıcılık gibi sebeplerle kullanıldığı için QR-Kod aracılığıyla yapılan ödemeleri durdurma kararı almıştır (Erdal, 2018).

Yukarıda bahsi geçen saldırıların yanında mevcut bir QR koda saldırmak için en kolay yol, orijinal QR kodu ile aynı tarzda manipüle edilmiş QR kod ile birlikte, yeni bir QR kod içeren bir çıkartma üretmektir. Bu yanıltıcı QR kodu ise, var olan orijinal kodun üzerine yerleştirmektir.

2.2.2. Güvenlik Önlemleri

Önceki bölümde bahsi geçen saldırılara karşı alınabilecek önlemlerin başında güvenlik zincirinin en zayıf halkası olan insanın sosyal mühendislik saldırılarına karşı daha dikkatli olması, kaynağı bilinmeyen QR kodları okutmamaları gerekliliği gelmektedir. Kullanıcının bir QR kodun güvenilirliği konusunda karar verme sürecine ilişkin araştırma zorluklarını vardır. QR kodlar insanlar tarafından okunamadığı için, kullanıcıya bilgi vermek için içerik gösterimi yapılabilir (Krombholz vd., 2014:79). Bunun yanı sıra QR kod okutmak için özel olarak geliştirilmiş güvenli QR kod okuyucuları kullanarak okutulan QR kodun güvenilirliği test edilebilir.

Kullanılan mobil cihazın işletim sisteminin güncel olması, güvenli QR kod okutmak için uygulama kullanımı alınacak önlemlerdendir. Günümüzde kullanılan birçok akıllı mobil cihaz kamerasında varsayılan olarak QR Kod okuyucu yüklü gelmektedir. Fakat mobil cihazda, ziyaret etmeden önce URL'yi kontrol etmeyi sağlayan bir QR Kod uygulamasına sahip olmak, kullanıcıya ziyaret etmek üzere olduğu URL'nin kaynağını doğrulama yeteneği vermektedir. Yanında herhangi bir bilgi bulunmayan QR Kodlar için bu güvenlik kontrolü mümkün değildir. Bu nedenle, tüm QR Kod okuyucu uygulamaları, bağlantıyı ziyaret etmeden önce, kullanıcıya kodu çözülmüş URL'yi göstermeli ve bağlantıyı ziyaret etmek isteyip istemediğini sorması gerekmektedir. Ayrıca, tarayıcılarda bulunan güvenlik göstergelerinin bazıları QR Kod okuyucu yazılıma gömülebilmektedir.

Güvenli bir QR kod sisteminde, (i) QR kod üreten yazılımda kimlik doğrulama mekanizmasının olması, veri bütünlüğünün sağlanması, (ii) çevrimiçi içeriğin doğrulanması

ve (iii) QR kodda olası zararlı içeriğin izole edilmesi gibi önlemleri içermesi gerekmektedir (Bani-Hani vd. 2014).

(i) QR kodun üretecinin doğrulanması ve veri bütünlüğünün test edilmesi olası Dolandırıcılık, SQL Enjeksiyonu, Komut Enjeksiyonu saldırılarına karşı önlem olacaktır. Kodun yaratıcısını doğrulamak ve böylece QR kodunun değiştirilip değiştirilmediğini kontrol etmek için dijital imzaların QR kod standardizasyonu ve entegrasyonu önemlidir. Dijital imza, saldırganın sağlama toplamını (checksum) ve buna göre doğrulama işleminde değişiklik yapması gerektiğinden, QR kod tabanlı saldırıları önemli ölçüde karmaşıklaştırır. Bununla birlikte, kodlanacak veri miktarındaki artış, gerçek verileri kodlayan alanı azaltır. Ayrıca, QR kod okuyucularının dijital imzaları doğrulayacak ve SSL'ye benzer şekilde doğrulamanın başarılı olup olmadığını belirtecek şekilde uyarlanması gerekir (Krombholz vd., 2014:79). QR kodun üretecinin doğrulanması ve veri bütünlüğünün test edilmesi amacı ile dijital imza algoritmalarının yanı sıra şifreleme ve özetleme algoritmaları da kullanılmaktadır.

(ii) QR kodlar ile karşılan en sık saldırı olan güvenilir olmayan URL'e yönlendirme sonucu; kimlik avı, zararlı yazılımın (virüs, solucan, truva atı) yayılması saldırılarına karşı çevrim içi içeriğin güvenilirliğinin test edilmesi gerekmektedir. QR kod okuyucu uygulamanın sahte ve gerçek URL ayrımını yapabilmesi gerekmektedir. QR kodun kötü niyetli URL içerip içermediğini tespit etmek için birçok uygulama önerilmiştir. Örneğin, QRphish API uygulamasının, tespit mekanizması olarak, %93,34 doğrulukla Phistank (Ulevitch,2006) gibi halka açık kara listesinden daha iyi ve algılama mekanizması %82,9 daha fazla URL saptama yeteneğine sahip olduğu bilinmektedir (Alnajjar vd., 2016:553).

(iii) Çalıştırılabilir kodların veya komutların QR kodu okutulan cihazın kaynaklarına ulaşmasını önlemek için QR kod içeriğinin izole edilmesi gerekmektedir. İçeriğin izole edilmesi ile gizliliğin ihlali, kişisel bilgilere ulaşma, okuyucu cihazın düzenlenecek DDOS ve Bot net gibi saldırılarda araç olarak kullanımı gibi saldırıların önüne geçilebilir. En basit yöntemi QR kod okuyucu uygulama dahil olmak üzere uygulamaların QR kod okuyucu cihazın (akıllı telefon, tablet) kaynaklarına (kamera, telefon rehberi, fotoğraflar, konum bilgileri vb.) erişimini engellemektir. Okuyucu uygulama izinleri, arabellek taşması, Komut ve SQL enjeksiyonu gibi çeşitli saldırıları başlatmak için de kullanılabilir.

Bunların yanı sıra QR kodun manipülasyonu saldırısına karşı alınabilecek önlem ise maskeleme yöntemi veya görsel QR kodlar olacaktır; teknik özelliklere uygun bir QR kodunda siyah beyaz modüllerin dağılımı, belirli bir modeli izler. Bu desen, dikkate alınan modülün renginin değiştirilip değiştirilmeyeceğini belirtmek için kullanılan maske tarafından belirlenir. Siyah ve beyaz modüllerin eşit dağılımından sapma ne kadar yüksekse, QR kodunun değiştirilme olasılığı o kadar yüksektir. Okuyucu uygulamayı güvenceye almak için maskeleme yöntemlerini kullanmak için hata oranı ve güvenlik arasındaki değişimin ayrıntılı bir analizi yapılmalıdır (Krombholz vd., 2014:79).

Ayrıca, son yıllarda, araştırmacılar QR kodu estetik unsurlarla donatmaya çalışmış ve görsel açıdan güzelleştirilerek, görsel algı bozulmasını en aza indirecek kod çözmesi kabul edilebilir yapıda kodlar formüle edilmiştir. Bu amaçla kod içindeki modüllerin şekli ve rengini değiştirilebilir veya bir resim QR koda gömülebilir (Lin vd. 2015:1015). Bu yöntem, değiştirilmiş QR kodlarını tespit etmede kullanıcıyı önemli ölçüde destekler. Tema ne kadar karmaşık olursa, bir saldırganın QR kodlarını göze batmayan bir şekilde değiştirmesi zorlaşır.

(a)

(b)

Şekil 2: (a) Modüllerin rengini ve şeklini değiştirme (b) Resim Gömme (Embedding a Picture) Kaynak: Lin vd. 2015: 1015

3. ARAŞTIRMA YÖNTEMİ

Çalışmada, insanların halka açık yerlerde bulunan QR Kodları taratmalarındaki motivasyonları ve QR Kodlar ile düzenlenen kimlik avı saldırına karşı farkındalık düzeyleri araştırılmıştır. Bu amaçla 3 farklı tipte QR kod afişi (Şekil 3) tasarlanmıştır. Bunlar; (i) Sade QR Kod afişi: üzerinde QR kodun kendisi hariç herhangi bir bilgi veya resim bulunmayan, (ii) Talimatlı QR Kod afişi: üzerinde QR kodun kendisi ve mobil telefon ile nasıl okutulacağı bilgilerinin yer aldığı, (iii) Resimli QR Kod afişi: üzerinde QR Kod ile birlikte bir görselin bulunduğu afiştir.

(a) *Sade QR Kod*

(b)*Talimatlı QR Kod*

Bu QR Kodu telefonunuza taramak için;
1)Akıllı telefonunuzun kamera uygulamasını açın. (Eğer "QR Kodları tarama" seçeneği etkin değilse lütfen kamera ayarlarından etkinleştirin.)
2)Akıllı telefonunuzu, QR Kodu kamera uygulamasına görünecek şekilde tutun. (Arka kamera açık olmalıdır.)
3)QR Kod ile ilişkili bağlantıyı açmak için ekranda çıkan bildirime tıklayın.
4)Eğer taratamadıysanız, Google Play Store veya Appstore'dan "QR Code Reader And Scanner" Kaspersky Lab kaynaklı olan uygulamayı indirip taratabilirsiniz.

(c-1) *Resimli QR Kod* ***(c-2)*** *Resimli QR Kod*

Şekil 3. QR Kod Afişleri (a-b-c)

Tasarlanan QR Kodlar, akıllı telefon ile taratıldığında, kullanıcıyı içerisinde çevrim içi anket bulunan bir web sitesine yönlendirmektedir. Anket çalışmasında Kapsalis'in (2013) QR Kod ölçeği birebir Türkçe'ye çevirilerek uygulanmıştır. Toplam 7 soru içeren anketin 2 sorusu katılımcının demografik bilgilerini, diğerleri ise QR kodu taratmadaki motivasyonu, taratırken herhangi bir şüphe duygusunun varlığı, ne sıklıkla QR kod tarattığı, daha önce bir saldırının kurbanı olup olmadığı yönünde bilgiler üzerinedir. "Google Forms" ile oluşturulan bu anket Tablo 1 de yer almaktadır.

Tablo 1. Anket soruları

Sorular	Şıklar
1- Bu QR Kodu neden taradınız?	a) Merak Ediyordum. b) İlgili bilgi beni çekti. c) Resim ilgimi çekti. d) Sıkılmıştım. e) QR Kodun ne olduğunu bilmiyorum. f) Cevap vermek istemiyorum. g) Diğer:.....
2- Bu QR Kodu taramadan önce herhangi bir şüpheniz veya kötü beklentiniz var mı?	a) Hayır, her şeyin güvenilir olduğunu düşündüm. b) Hayır, hiç düşünmedim. c) Evet, biraz garip görünüyordu. d) Evet, her zaman şüpheliyim.
3- Bir QR Kodu tararken, bağlantıyı ziyaret etmeden önce web adresini kontrol ediyor musunuz?	a) Evet. b) Hayır, çünkü QR Kod okuyucum otomatik olarak bağlantıyı ziyaret ediyor. c) Hayır. d) Web adresini nasıl kontrol edebileceğimi bilmiyorum. e) Kontrol edip etmediğimi hatırlayamıyorum.
4- Hiçbir kimlik avı saldırısının kurbanı oldunuz mu?	a) Evet. b) Emin değilim. c) Hayır, ama tanıdığımızın başına geldi. d) Hayır. e) Kimlik avı saldırısının ne olduğunu bilmiyorum. f) Cevap vermek istemiyorum.
5- QR Kodlarını ne sıklıkla tarıyorsunuz?	a) Ne zaman görsem. b) Çok sık. c) Nadiren. d) Neredeyse hiç.
6- Cinsiyetiniz ne?	a) Erkek. b) Kadın. c) Cevap vermek istemiyorum.
7- Yaşınız nedir?	a) 18 yaşın altında. b) 18 – 24. c) 25 – 30. d) 31 – 45. e) 46 – 60. f) 61 ve üstü. g) Cevap vermek istemiyorum.

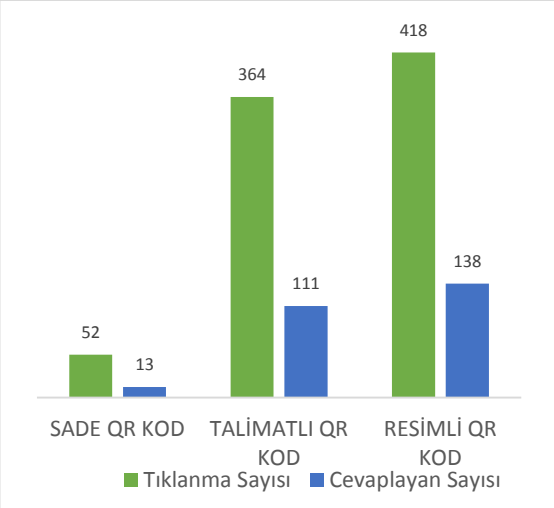
Araştırma kapsamında, teknoloji okuryazarlığı bulunan eğitimli genç nesil hedef kitle olarak belirlenmiş, Ankara ilinde bulunan üniversite ve teknokentlere başvurular yapılmıştır. Başvurulara olumlu yanıt veren Başkent Üniversitesi'nin ve Hacettepe Teknokent'in belirlenen alanlarında veri toplama süreci gerçekleşmiştir

Tasarlanan QR kod afişleri Başkent Üniversitesi Bağlıca Kampüsünde yer alan servis durakları, kafeteryalar, yemekhaneler, kırtasiye-fotokopi kısımları, market vb. yerlerdeki duyuru panolarına asılmıştır. Ek olarak, bünyesinde 267 adet firma bulunan Ankara Hacettepe Teknokent duyuru panolarına QR Kod afişleri yerleştirilmiştir. Her bir tipten (Sade, Talimatlı ve Resimli) eşit sayıda olacak şekilde toplamda 60 adet QR kod afişi 40 gün (3 Ekim 2019-11 Kasım 2019) süresince belirtilen yerlerde asılı kalmıştır.

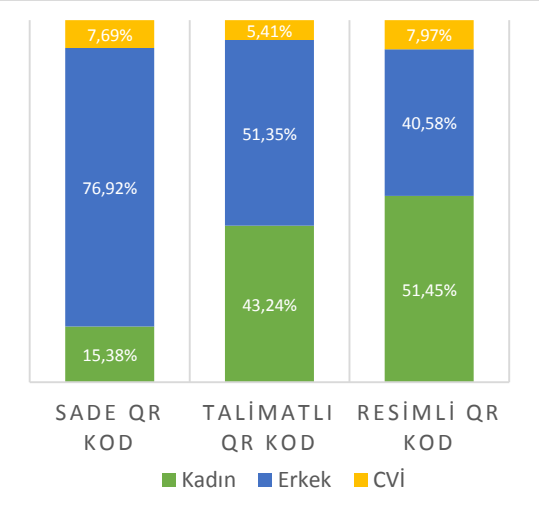
4. ANALİZ VE BULGULAR

Önceki bölümde detayları verilen QR Kod afişlerinin yönlendirdiği web adresine toplamda 834 kişi tarafından tıklanmış fakat 262 kişi (%31,41) anketi cevaplamıştır. Ayrıca QR kod afişlerini tarattığı halde ilgili web adresine girmeyenlerin sayısı bilinmemektedir.

Tıklanma sayısı ve anketi cevaplayan sayısını gösteren Şekil 4'te; sade QR Kod afişinin yönlendirildiği web adresi 52 kişi (%6,24) tarafından tıklanmış ama anketi cevaplayan kişi sayısı 13'tür (%1,56). Talimatlı QR Kod için tıklayan sayısı 364 kişi (%43,65), cevaplayan sayısı 111 kişidir (%13,31). Resimli QR Kod için tıklanma sayısı 418 kişi (%50,12), anketi cevaplayan sayısı ise 138 kişidir (%16,55). 572 kişinin (%68,59) anketi görüp doldurmadığı görülmektedir.



Şekil 4. Tıklanma ve Anket Cevaplanma sayısı



Şekil 5. Cinsiyet Dağılımı

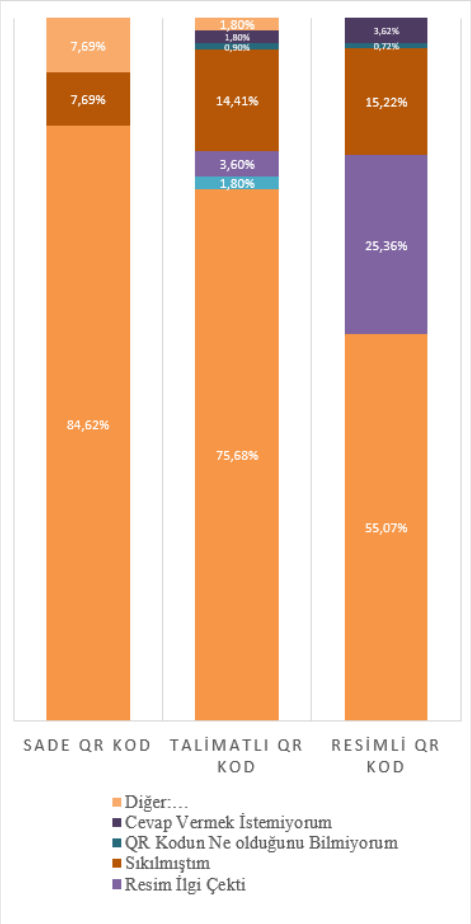
Katılımcıların cinsiyet grafiği Şekil 5'de verilmiştir. Ankete katılanların cinsiyetleri Kadın (121) ve Erkek (123) sayılarının toplamda hemen hemen eşittir. Bu soruya cevap vermek istemeyenlerin (CVİ) sayısı ise toplamda 18 kişidir. Detaylı incelendiğinde cinsiyetler arası fark en yüksek sade QR kodda olduğu görülmektedir. Sade QR Kodu taratan erkek sayısı kadın sayısından %61.54 fazladır. Bunun yanı sıra Talimatlı QR kodu taratan Erkek sayısı Kadın sayısından % 8,11 fazla iken Resimli QR Kodu taratan Kadın sayısı Erkek Sayısından

%10,87 fazladır. Kadın katılımcılar parti ve para görsellerini içeren Resimli QR kodu daha fazla tercih etmişlerdir.

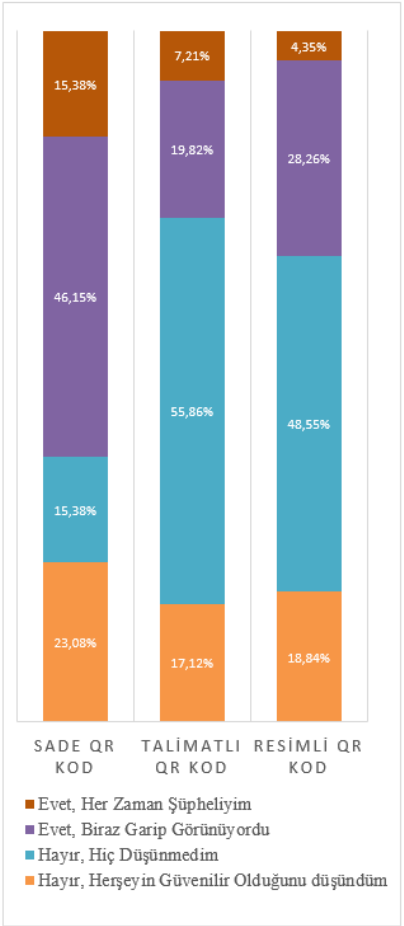
Ankete katılanların %82 si 18-24 yaş aralığında iken % 0,7'si ise 45 yaş üzeridir. Tüm QR Kod afişleri için 18-24 yaş aralığında katılım en yüksektir. Sade QR Kod afişini 18 yaş altı ve 30 yaş üzeri kimse taratmamıştır. 30 yaş üzeri katılımcıların %76'sı Resimli QR Kodu taratırken %24 ü talimatlı QR kodu taratmıştır.

QR kodu taratan kişilerin motivasyonunu öğrenmek için sorulan "Bu QR Kodu neden taradınız?" sorusuna verilen cevaplar (Şekil 6) bireylerin merak duygularının ön planda olduğunu göstermektedir. QR kod afişlerine yerleştirilen resimlerin kişilerin merak duygusunu arttırdığı afişin taratılma sayısı ile de desteklenmektedir. Ayrıca resimli QR Kod anketini dolduran kişilerin %25'i resmin ilgisini çektiğini belirtmiştir. Toplamda ankete katılanların %14,5'i ise sıkıldığı için ilgili afişi tarattığı bilgisini vermiştir.

Anketi dolduran kişilerin farkındalık düzeyini belirlemek için yöneltilen "Bu QR Kodu taramadan önce herhangi bir şüpheniz veya kötü beklentiniz var mı?" sorusuna verilen cevaplar Şekil 7'de sunulmuştur. Bu soruya katılımcıların %68,3 ü hayır cevabı ile şüphe duymadığını %31,7 si ise Evet cevabı ile şüpheli yaklaştığını belirtmiştir. Bunun yanı sıra Sade QR kod Afişinin diğerlerine göre daha fazla şüphe uyandırdığı görülmektedir.

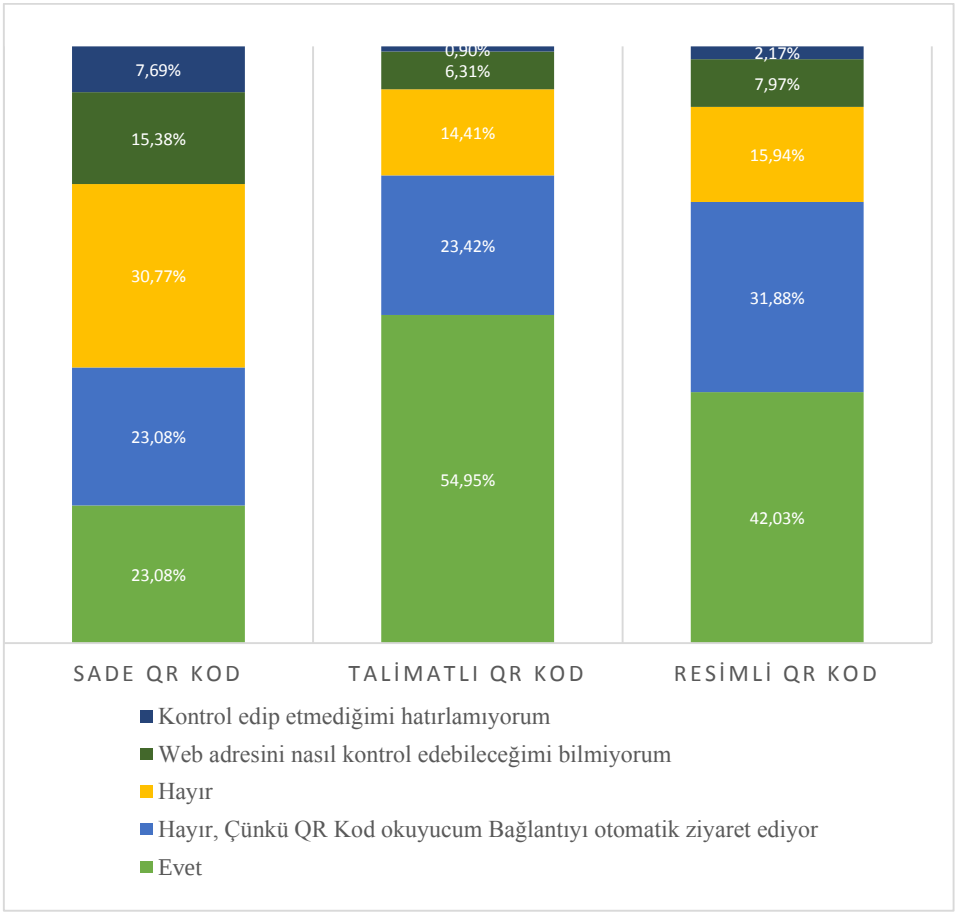


Şekil 6. Katılımcıların QR Kod afişlerini taratma motivasyonu



Şekil 7. Katılımcıların şüphe veya kötü beklenti oranları

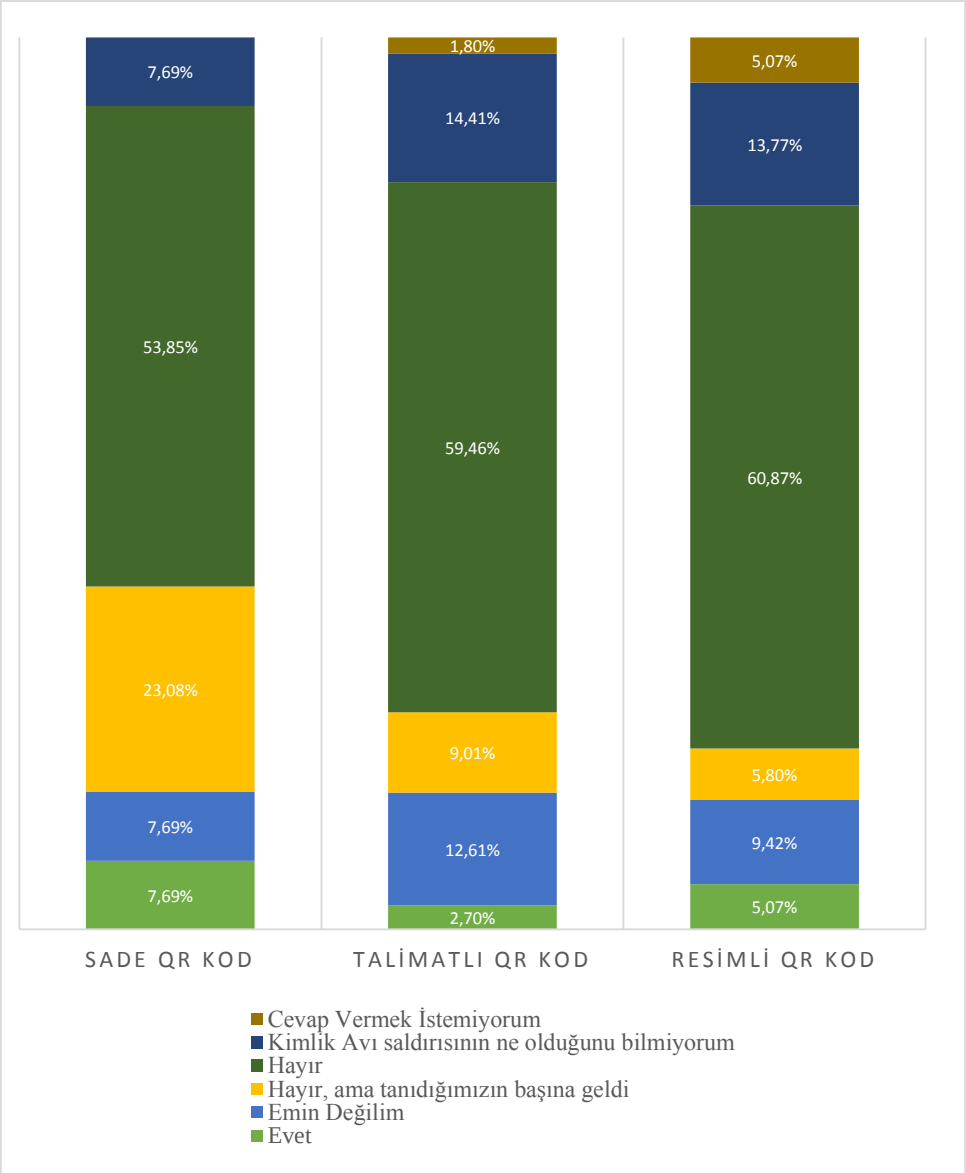
Katılımcılara bir QR Kodu tararken, bağlantıyı ziyaret etmeden önce web adresini kontrol edip etmedikleri sorulduğunda ise tüm afişler için toplam %46,6 kontrol ettikleri şıkkını işaretlerken, web sayfasının otomatik açılması veya nasıl kontrol edileceğinin bilinmemesi gibi farklı sebeplerden %51,5 web adresini kontrol etmediklerini belirtmişlerdir. Kalan %1,9 katılımcı ise kontrol edip etmediklerini hatırlamamaktadır.



Şekil 8. Katılımcıların Web adresi kontrolü yapma yüzdeleri

Ankete katılan katılımcıların toplamda % 59,9 unun daha önce bir kimlik avı saldırısının kurbanı olmadıklarını % 4,2 ise bu saldırıyı kurban olarak tecrübe ettiklerini belirtmiştir. QR Kod afiş tipine göre verilen cevapların yüzdeleri Şekil 9 da verilmiştir.

Çalışmada, kullanım alanının günümüzde hızla arttığı QR Kodların, ne sıklıkla taratıldığı da incelenmiştir. Katılımcıların %16,41'i ne zaman görse ve %10,69'u çok sık tarattığını belirtirken %57,25 nadiren ve %15,65'i ise neredeyse hiç taratmadıklarını belirtmiştir.



Şekil 9. Katılımcıların "kimlik avı saldırısına uğrama" sorusuna ilişkin değerlendirmeleri

Bu çalışmadaki sonuçlar analiz edilirken Mobil cihazların işletim sistemleri ve versiyonları da incelenmiştir. Mobil cihazlarda toplamda %74,2 IOS işletim sisteminden %25,8 Android işletim sisteminden giriş yapılmıştır. Google Analitik verilerine göre, 11 farklı IOS (en güncel versiyon 13.1.3 ve en düşük versiyon 10.3.3) versiyonu ve 47 farklı Android (en düşük 5.0 (Lollipop) ile en güncel Android 10 (One UI 2.0 tabanlı)) versiyonu tespit edilmiştir. 30 farklı web tarayıcısı sürümü tespit edilmiştir.

Dışarıdan yazılım yüklemeye izin veren tek ve dünyanın en popüler mobil işletim sistemi Android, bu özelliğinden dolayı mobil kötü amaçlı yazılımlarının başını çeken Trojan tehditlerine açıktır. Bu sebeple Android mobil cihazlarda virüsten koruma, casus yazılım önleyici çeşitli güvenlik uygulamaları daha yaygın olarak kullanılmaktadır (Örn: Eset Mobile Security). IOS işletim sistemi her ne kadar en güvenli işletim sistemi olarak kabul görse de, verileriniz ve değerli bilgileriniz için, dışarıdan gelebilecek tehlikelere karşı koruyamayabilir. Son zamanlarda, IOS içinde güvenlik yazılımları çıkmıştır. (Örn: Norton Mobile Security ve

Kaspersky Security Cloud). Katılımcıların herhangi bir güvenlik uygulaması kullanıp kullanmadıkları araştırma kapsamı dışındadır fakat çoğunluğun daha güvenli olarak kabul edilen IOS işletim sistemini kullandıkları tespit edilmiştir.

5. SONUÇ VE DEĞERLENDİRME

QR kodlar, İnternet ve akıllı telefonların hızla yaygınlaşması ile hayatımızın her alanında yer almaya başlamıştır. Bankacılık uygulamaları, ilanlar, kartvizitler, reklamlar, ürün takibi bunlardan sadece bir kaçıdır. Uygulama alanının bu kadar geniş oluşu, insanların QR koda karşı yapılabilecek saldırılardan habersiz oluşları, QR kodun içindeki verilerin insan gözüyle görülememesi, veri saklama kapasitesinin yeterli oluşu, QR kodu saldırıların odak noktası haline getirmektedir.

QR kod ile düzenlenebilecek saldırılar; SQL ve Komut Enjeksiyonu, Kimlik Avı, Dolandırıcılık/Sahtecilik, Kötü amaçlı yazılımın (virüs, solucan, casus yazılım, Truva atı, vb.) yayılımı olarak sıralanabilir. Bu saldırıların, kullanıcıların kişisel verilerine ulaşılması, QR kod okuyucu cihazlarının kaynaklarının izinsiz kullanımı veya kullanım dışı kalmaları, kullanıcıların farkında olmadan başka saldırılara aracılık etmeleri gibi büyük maddi ve manevi kayıplara yol açabilir.

Bu çalışmada, teknoloji okur-yazar genç neslin QR Kodların olası güvenlik zafiyetleri ve yarattığı güvenlik sorunları ile bu konu hakkındaki farkındalık seviyeleri araştırılmıştır. Bir sosyal mühendislik deneyi olarak bakıldığında bu çalışma ile farklı lokasyonlara yerleştirilen QR Kod afişleri ile 834 kişinin yönlendirilen web adresini ziyaret etmeleri sağlanmıştır. Bu durum, QR Kod ile kimlik avı saldırı senaryosu kötü amaçlı düzenlenmiş olsaydı, 834 kişinin bu saldırının kurbanı olabileceğini göstermektedir. Kaynağı belli olmayan bir QR Kodun bu kadar fazla taratılması, genç neslin QR kodlardan kaynaklanan bir saldırıya karşı farkındalık düzeyinin oldukça düşük olduğunu göstermektedir. Aynı zamanda, katılımcıların çoğunun şüpheleri olsa bile bir QR Kodunun nereye yönlendirdiğini keşfetmeye meraklı olduğu ve QR Kod afişlerinde yer alan resim veya yazının kişilerin merak duygusunu arttırdığı görülmüştür. Kimlik avı saldırılarında QR Kod kullanımının çok yaygın olmaması bu alanda farkındalık seviyesini de düşürmektedir. Farkındalığın ve bilinirliğinin düşük olması saldırganların bu tür saldırılardan başarı elde etmesini kolaylaştırmaktadır. Bu sebeple, bilinirliği oldukça yüksek olan e-posta yolu ile kimlik avı saldırılarının yerini QR Kod ile yapılan saldırıların alabileceği öngörülmektedir.

Kullanıcıların eğitilmesi, güvenlik sorunlarının üstesinden gelmenin en etkili ve aynı zamanda en zor (pahalı ve zaman alan) yoludur. Rastgele bir QR Kodu taratmanın ve yönlendirdiği URL'yi ziyaret etmenin, belirsiz ve bilinmeyen bir etki alanını ziyaret etmekle tamamen aynı olduğunu fark etmek son derece önemlidir. Bir URL'nin yalnızca adına bakarak kötü amaçlı olduğunu doğrulamak oldukça zordur ancak ilk aşamada kullanıcılara; kaynağını bilmedikleri QR Kodları taratmamaları, gizli URL'leri ziyaret etmekten kaçınmaları ve doğrulanmamış kaynaklara hassas ve kişisel bilgiler vermemeye özen göstermeleri bilinci verilmelidir. Bu bilinçle, günümüzde özellikle genç neslin otomatikleştirilmiş özelliklere daha fazla güvenme eğilimleri ile güvenli QR Kod tarayıcı mobil uygulamaları kullanımı yaygınlaştırılabilir. Ek olarak, kullanılan akıllı mobil cihazın web tarayıcısı ve işletim sisteminin güncel versiyonlarının yüklenmesi ve QR kod üreten yazılımların kimlik

doğrulama mekanizmasının olması, veri bütünlüğünün sağlanması, çevrimiçi içeriğin doğrulanması ve QR kodda olası zararlı içeriğin izole edilmesi güvenlik seviyesini arttırmada etkili olacaktır.

KAYNAKÇA

Ahuja, S. (2014). QR Codes And Security Concerns. *International Journal of Computer Science and Information Technologie*s, *5*(3), 3878-3879.

Alnajjar A. Y., Anbar M., Manickam S., Elejla O., ve El-Taj H., (2016) . QRphish: An Automated QR Code Phishing Detection Approach. *Journal Of Engineering And Applied Sciences, 11*(3), 553-560, doi: 10.3923/jeasci.2016.553.560.

Al-Khalifa, H. S. (2008, July). Utilizing QR Code and Mobile Phones for Blinds and Visually Impaired People. In International Conference on Computers for Handicapped Persons (pp. 1065-1069). Springer, Berlin, Heidelberg.

Bani-Hani, R. M., Wahsheh, Y. A., & Al-Sarhan, M. B. (2014, November). Secure QR Code System. *In 2014 10th International Conference on Innovations in Information Technology (IIT)* (pp. 1-6). IEEE.

DHA, (2017). *Kod Yöntemiyle Dolandırıcılık Yapan Zanlı Tutuklandı*. Hürriyet Gazetecilik ve Matbaacılık A.Ş. [Çevrimiçi]. Erişim Adresi: http://www.hurriyet.com.tr/kod-yontemiyle-dolandiricilik-yapan-zanli-tutuk-40557306. Erişim Tarihi: 10.11.2019.

Elçi, A. (2014). *İş Ekipmanlarında Güvenlik Takibi İçin Bir Sistem Önerisi Karekod Barkod Uygulama*. Yüksek lisans tezi, İş Sağlığı ve Güvenliği Bölümü, Sağlık Bilimleri Enstitüsü, İstanbul Yeni Yüzyıl Üniversitesi, İstanbul, Türkiye.

Erdal, E. (2018). Çin Dolandırıcılığı Önlemek için QR Kod Ödemelerini Durduruyor İndirilme Tarihi: 01.10.2019 URL: https://www.webtekno.com/cin-dolandiriciligi-onlemek-icin-qr-kod-odemelerini-durduruyor-h38598.html.

Göksel, B. ve Başaran, A. (2016). QR-Code'daki Olta Bir Farkındalık Deneyi ve Qr Kodların Sosyal Mühendislik Saldırılarında Kullanılması. İndirilme Tarihi: 10.01.2020 URL: https://www.slideshare.net/AlperBasaran/qr-codelardaki-tehlike Rapor

Juniper Research (2018). Mobile Qr Code Coupon Redemptions to Surge, Surpassing 5.3 Billion By 2022. İndirilme Tarihi: 10.01.2020. URL: https://www.juniperresearch.com/press/press-releases/mobile-qr-code-coupon-redemptions-to-surge

Kapsalis, I. (2013). *Security of QR Codes*. Yüksek lisans tezi, Security and Mobile Computing, Department of Telematics, Norwegian University of Science and Technology, Trondheim, Norveç.

Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., Schrittwieser, S., Sinha, M., & Weippl, E. (2010, November). QR code security. *In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedi*a (pp. 430-435).

Koygun, P. Ç. (2018). *Dolandırıcılıkta Yeni Yöntem QR Kod*. CNNTurk. İndirilme Tarihi: 10.11.2019 URL:https://www.cnnturk.com/video/turkiye/dolandiricilikta-yeni-yontem-qr-kod.

Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014, June). QR code security: A Survey of Attacks and Challenges for Usable Security. *In International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 79-90). Springer, Cham.

Lin, S. S., Hu, M. C., Lee, C. H., & Lee, T. Y. (2015). Efficient QR Code Beautification with High Quality Visual Content. *IEEE Transactions on Multimedia*, *17*(9), 1515-1524.

Moharil, B., Ghadge, V., Gokhale, C., & Tambvekar, P. (2012). An Efficient Approach for Automatic Number Plate Recognition System Using Quick Response Codes. *IJCSIT*, 3(0975-9646), 5108-5115.

Polat, Z. A. (2014). Karekod Teknolojisinin Mesleğimizdeki Olası Kullanımları Üzerine Düşünceler. *V. Uzaktan Algılama-CBS Sempozyumu (UZAL-CBS 2014)*, İstanbul, Türkiye, 1-8.

Sharma, V. (2012). A Study of Malicious QR Codes. *International Journal of Computational Intelligence and Information Security*, *3*(5), 21-26.

Top, T. (2012). *Tribünde barkod pankart açanlar aranıyor*. Milliyet Gazetecilik ve Yayıncılık A.Ş., [Çevrimiçi]. Erişim Adresi: http://www.milliyet.com.tr/skorer/tribunde-barkod-pankart-acanlar-araniyor-1496180 Erişim Tarihi: 10.11.2019.

Ulevitch, D., "Phistank (OpenDNS)", (2006). İndirilme Tarihi: 17.10.2019 URL: https://www.phishtank.com/.

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013, April). QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. *In International Conference on Financial Cryptography and Data Security* (pp. 52-69). Springer, Berlin, Heidelberg.

Wane, A. R., Jamankar, S. P., & Chandure, O. V. (2013). An Effective Mechanism for Ensuring Security Of QR Code. *International Journal of Advanced Research in Computer Science*, *4*(6), 175-179.

Yin, L. R., Senior, M., Zhang, Z., & Baldwin, N. (2013, June). Perceived security risks of scanning quick response (QR) codes in mobile computing with smart phones. *In 2013 International Conference on Engineering, Management Science and Innovation (ICEMSI)* (pp. 1-7). IEEE.