BAŞKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

YÖNETİM BİLİŞİM SİSTEMLERİ YÜKSEK LİSANS PROGRAMI

QR KOD GÜVENLİK FARKINDALIĞI ÜZERİNE ANKARA İLİNDE BİR ARAŞTIRMA

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

MERT OGÜN BİLİR

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ ESMA ERGÜNER ÖZKOÇ

ANKARA - 2020

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Yönetim Bilişim Sistemleri Anabilim Dalı, Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı çerçevesinde "Mert Ogün Bilir" tarafından hazırlanan bu çalışma, aşağıdaki jüri tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 02 / 01 / 2020

Tez Adı: QR Kod Güvenlik Farkındalığı Üzerine Ankara İlinde Bir Araştırma

Tez Jüri Üyeleri (Unvanı, Adı - Soyadı, Kurumu)	**İmza**
Dr. Öğr. Üyesi Esma Ergüner ÖZKOÇ, (Danışman) Başkent Üniversitesi	....
Doç. Dr. Erdem KIRKBEŞOĞLU, Başkent Üniversitesi	....
Doç. Dr. Şule Erdem TUZLUKAYA, Atılım Üniversitesi	....

ONAY
Prof. Dr. İpek KALEMCİ TÜZÜN
Sosyal Bilimler Enstitüsü Müdürü
Tarih: … / … / ………

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 22/12/2019

Öğrencinin Adı, Soyadı: Mert Ogün Bilir

Öğrencinin Numarası: 21710225

Anabilim Dalı: Yönetim Bilişim Sistemleri Anabilim Dalı

Programı: Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı

Danışmanın Unvanı/Adı, Soyadı: Dr. Öğr. Üyesi Esma Ergüner Özkoç

Tez Başlığı: QR Kod Güvenlik Farkındalığı Üzerine Ankara İlinde Bir Araştırma

Yukarıda başlığı belirtilen Yüksek Lisans tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 70 sayfalık kısmına ilişkin, 22/12/2019 tarihinde şahsım/tez danışmanım tarafından turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 6'dır. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası: M.O.B.

ONAY

Tarih: 22/12/2019

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Dr. Öğr. Üyesi Esma Ergüner Özkoç

....

TEŞEKKÜR

Öncelikle yüksek lisans öğrenimim sırasında destek ve yardımlarını hiçbir zaman esirgemeyen danışman hocam; Dr. Öğr. Üyesi ESMA ERGÜNER ÖZKOÇ'a teşekkür ederim. Değerli tecrübe ve bilgilerini benimle paylaşan ve bana zaman ayıran Saygıdeğer hocam; Doç. Dr. Erdem KIRKBEŞOĞLU'na teşekkür ederim. Yüksek lisans eğitimim boyunca katkılarını esirgemeyen saygıdeğer hocalarım; Prof. Dr. Ali HALICI, Doç. Dr. Murat Paşa UYSAL, Öğr. Gör. Gülten GÜNGÖRMÜŞ ve Öğr. Gör. Gizem ÖĞÜTÇÜ'ye teşekkür ederim. Ayrıca tez çalışmam sırasında bana sürekli destek olan aileme ve çalışma arkadaşlarıma teşekkürlerimi sunarım.

ÖZET

Mert Ogün BİLİR, QR Kod Güvenlik Farkındalığı Üzerine Ankara İlinde Bir Araştırma, Başkent Üniversitesi Sosyal Bilimler Enstitüsü, Yönetim Bilişim Sistemleri, 2019

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, bankacılık, eğitim, nesne tanımlama, ürün izleme vb.) yayılmıştır. QR Kod kullanımı, kolay üretilişi ve dağıtımı, geniş depolama kapasitesi ve hızlı okunabilirliği nedeniyle hızla yaygınlaşmıştır. 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 bir çevrimiçi anket uygulanmıştır. Teknolojiyi okur-yazarı ve yeni teknolojilere adaptasyonu hızlı olan genç nesil hedef kitle olarak seçilmiştir. Çalışma kapsamında üç farklı QR Kod (Sade, Talimatlı ve Resimli) tasarlanarak afişler hazırlanmıştır. Bu afişler Başkent Üniversitesi Bağlıca Kampüsündeki ve Hacettepe Teknokent'teki birçok panoda 40 gün süresince asılı kalmıştır. QR Kodları taratan kullanıcılar çevrimiçi anketin bulunduğu web bağlantısına yönlendirilmektedir.

834 kişi QR Kod afişlerinin yönlendirdiği web adresini ziyaret etmiş, çevrimiçi anket ise 262 kişi tarafından cevaplanmıştır. Anket cevaplarından toplanılan veriler, kullanıcıların QR Kodu taratma motivasyonlarının esas olarak merak duygusundan ileri geldiğini göstermektedir. Bunun yanı sıra kullanıcıların potansiyel tehditler ve kendilerini koruma yolları hakkında bilgi eksikliğine sahip oldukları sonucuna varılmıştır. Ayrıca bir sosyal mühendislik deneyi olarak da düşünülebilecek bu çalışma sonunda QR Kod ile düzenlenen saldırılar ve bu saldırılara karşı alınabilecek önlemler de sunulmuştur.

Anahtar Kelimeler: QR Kod, Kimlik Avı saldırıları, QR Kod güvenliği.

ABSTRACT

Mert Ogün BİLİR, A Research on QR Code Security Awareness in Ankara, Başkent University Institute of Social Sciences, Management Information Systems, 2019

The QR codes (Quick Response Code), which were first used in the production area in 1994, have spread to 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, an online questionnaire has been applied on determining the level of awareness of individuals about possible security weaknesses of QR Codes in social life and the problems they will create. The young generation, who technology literate and has a fast adaptation to new technologies, has been chosen as the target.Within the scope of the study, three different QR Codes (Plain, Instructional and Illustrated) were designed and posters were prepared. These posters were hung for 40 days in many boards in Başkent University Bağlıca Campus and Hacettepe Technopolis. Users who scan QR Codes are directed to the web link where the online survey is located.

834 people visited the web address directed by the QR Code posters and the online questionnaire was answered by 262 people. The data collected from the questionnaire answers demonstrates that the motivations of users to scan the QR Code are mainly due to curiosity. In addition, it is concluded that users have a lack of information about potential threats and ways to protect themselves. At the end of this study, which can also be considered as a social engineering experiment, the attacks organized with QR Code and the measures that can be taken against these attacks are presented.

Keywords: QR Code, Phishing Attack, Security of QR Codes.

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

KISALTMALAR LİSTESİ

BT	Bilişim Teknolojileri
CSS	Cascading Style Sheets (Basamaklı Stil Sayfası)
dB	Desibel
dBi	Anten Kazancı Miktar Ölçüsü
DDOS	Denial-Of-Service Attack
DWT	Discrete Wavelet Transform
EAN/UPC	European Article Numbering / Uniform Products Code
GHz	Gigahertz
Ltd. Şti.	Limited Şirketi
HTML	Hyper Text Markup Language (Hiper Metin İşaretleme Dili)
IBM	International Business Machines
IP	Internet Protocol Address
JPEG	Joint Photographic Experts Group
MIS	Management Information Systems
MICR	Magnetic Ink Character Recognition (Manyetik Mürekkep Karakter Tanıma Kodu)
OCR	Optical Character Recognition
OTP	One Time Password (Tek Seferlik Parola)
OT/VT	OT/VT Otomatik Tanıma ve Veri Toplama (Automatic Identification and Data Capture)
OR	Veya
ÖSYM	Ölçme, Seçme Ve Yerleştirme Merkezi
Örn	Örneğin

QR Kod	Quick Response Code (Karekod)
QRLJacking	QR Code Login Jacking
RF/ID	Radio Frequency Identification (Radyo Dalgaları ile Tanıma)
RF/DC	Radyo Dalgaları ile Veri İletişimi
SQL	Structured Query Language
SSL	Secure Sockets Layer (güvenli giriş katmanı)
URL	Uniform Resource Locator
WAN	Wide Area Network (Geniş Alan Ağı)
vb.	Ve benzeri
vd.	Ve diğerleri
XSS	Cross Site Scripting
YBS	Yönetim Bilişim Sistemleri

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 aktarabilmekte ve depolayabilmektedirler (Elçi, 2014: 10). 1994 yılında Denso Wave firması tarafından otomobil endüstrisinde kullanılmak için geliştirilen QR Kodu, kolay üretilişi ve dağıtımı, depolama kapasitesi ve hızlı okunabilirliği nedeniyle popüler olmuştur.

QR Kodlar günümüzde sıklıkla kullanıcıları daha fazla bilgi veya hizmet sağlayabilecek ilgi alanlarına yönlendiren web sitelerine yönlendirmek için kullanılmaktadır. Bunun yanı sıra birçok farklı uygulamada QR Kodlar kullanılmaktadır. Bunlardan, otomatik plaka tanıma sisteminde (Moharil ve Diğerleri, 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 belgelere kolay ulaşım ve kullanım kolaylığı sağlanmaktadır (Elçi, 2014: 29-40). Pazarlama endüstrisinde ise QR Kodları reklamcılığın tamamlayıcı bir yolu olarak kullanılmaktadır. Bir reklam, müşteriyi ürünle ilgili ek bilgilerin bulunduğu web sayfasına götürebilmektedir. 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: 1065-1069) 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 Kodu okutarak, 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 Kodunda kodlanan bilgileri taramadan önce bilmemeleridir. Örneğin; stada küfürlü pankart sokamayan Karşıyaka taraftarlarının Göztepe derbisinde küfür içeren bir URL'e yönlendiren QR Kod pankartı, polis aramasını kolaylıkla geçmiştir (Milliyet Gazetecilik ve Yayıncılık A.Ş., 2012). Bu gibi farklı sebeplerle, saldırganlar çeşitli saldırı türleri için QR Kodlarını kullanmaktadır (Shin ve Yao, 2013: 49). Bunlara ek olarak saldırganlar QR Kodun okutulduğu cihazda kaydedilmiş özel verilere ulaşılabilmekte, kaydedebilmekte ve değişiklik yapabilmektedir. Akıllı telefonların güvenlik düzeyinin arttırılması, kullanıcının mahremiyetinin korunması ve farkındalığının arttırılması amacı ile önlem alınması gerekmektedir.

Çalışmanın amacı; algılanan QR Kod güvenlik riskini ve bunun nasıl azaltılacağı üzerine kullanıcıların bu konudaki farkındalığını araştırmaktır. Bu araştırmada yöntem olarak, kötü niyetli QR Kodlarının uyarılarına nasıl yanıt vereceğini belirlemek için çevrimiçi bir anket uygulanmıştır. Kişilerin QR Kod kullanımına karşı risk algıları ve karşılaşabilecekleri önlemlere değinilmiştir.

Anket sonuçları, bilgisayar ve teknolojide daha fazla deneyime sahip olan kullanıcıların, uyarı mesajlarını görmezden gelmelerinin daha muhtemel olduğunu ve kullanıcıların çoğunluğunun, QR Kod riskleri konusunda düşük düzeyde farkındalığa sahip olduğunu göstermektedir. İnsanların kaynağını bilmedikleri bir QR Kodu neden okuttuğu sorgulandığında ise temel sebebin merak duygusu olduğu ortaya çıkmaktadır. Bunun yanı sıra teknik açıdan değerlendirildiğinde; bir QR Kodun (versiyon 40) içerebileceği en fazla binary (ikili sayı sistemi) 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 ve diğerleri, 2010: 2). Bu durumda bir QR Kod, saldırı yapmak isteyen kötü niyetli kişiler için hem insani hem de teknik açıdan yeteri kadar cezbedicidir. Henüz okunduğunda tüm sistemi yok edecek bir QR Kod geliştirilmemiş olması, QR Kodun potansiyel bir tehdit olduğu gerçeğini değiştirmemektedir.

QR Kod, kolay üretilmesi dağıtılması ve içerdiği veri miktarı fazla olması sebebiyle popülerdir. QR Kodlar, düz metin içeren bir sayfa veya bir web sitesine yönlendirmektedirler. Mobil ödeme için kullanılabilmektedir. Kullanıcılar, bir kimlik avı web sitesi (phishing) veya bir kötü amaçlı yazılım dağıtıcı gibi zararlı bir web sitesine yönlendirebilmektedir (Shin ve Yao, 2013: 49). Bunun yanı sıra; SQL ve komut enjeksiyonu, QRLJacking, tarayıcı tabanlı saldırılar yapılabilmektedir. Ek olarak, orijinal bir QR Kod değiştirilerek sahte QR Kod oluşturulabilmektedir. Böylelikle, kullanıcı adı, şifre, kredi kartı bilgileri gibi vb. hassas bilgileri ele geçirilebilmektedir. Bu gizli ve hassas bilgiler, kötü niyetli kişilerin eline geçmesiyle birlikte kullanıcılar maddi veya manevi zarara uğramaları mümkündür.

Söz konusu riskler, yeni bilgi kodlama teknolojisi üzerinde daha fazla araştırma yapılmasını gerektirmektedir. Bu sebeple çalışmada QR Kod ile yapılabilecek saldırılar araştırılmış ve saldırılara karşı alınabilecek önlemler sunulmuştur.

Çalışmanın temel araştırma sorusu toplumsal yaşamda bireylerin QR Kodların olası güvenlik zafiyetleri ve yaratacağı sorunlar hakkındaki farkındalık seviyelerinin tespit edilmesi üzerinedir.

Çalışmanın ilk bölümünde QR Kodun yapısı, ikinci bölümünde QR Kod saldırıları, üçüncü bölümünde QR Kod saldırılarına karşı alınabilecek önlemler, dördüncü bölümünde QR Kodun güvenlik farkındalığı ölçmek amacıyla yapılan araştırma yöntemi, beşinci bölümde analiz ve bulgular, altıncı bölümde ise sonuç ve değerlendirme yer almaktadır.

I. BÖLÜM: QR KODUN YAPISI

1.1. QR Kod Nedir?

QR Kod (Quick Response), orijinal adı “datamatrix” tir. Beyaz zemin üzerine siyah şekil ve motiflerden oluşan bir karedir. Diğer bir ifadeyle, bilgileri kodlamak için kullanılan iki boyutlu matris barkodlarıdır. Herhangi bir otomobilin, cihazın, derginin, kutunun veya ürünün üzerinde verilmesi gereken bilgilerin konumlandırılması ve bunların o alana sığdırılması zor olabilmektedir. Bu nedenle ürünün veya kutunun üzerinde karekod uygulamaları geliştirilmiştir. Karekod, QR okuyucular veya mobil okuyucu cihazlar tarafından okunduğunda, kodlanan bilgiye erişilmekte veya ilgili internet sitesine yönlendirme yapmaktadır (Elçi, 2014: 10).

1.2. QR Kodun Kullanım Alanları Nelerdir?

Eğitim alanında, öğrenci devam kayıt sisteminde QR Kod kullanılmaktadır. Öğrencilerin derse devam ettiklerini onaylaması için QR Kodu taraması gerekecektir. Ayrıca öğrenci kimliği doğrulaması da yapılmaktadır. Bu sistem, derste klasik yöntemle alınan yoklama sisteminin dersi etkilememesi ve zaman kaybının ortadan kaldırılması için kullanılabilir (Masalha ve Hirzallah, 2014: 75). Ayrıca Hendry ve diğerleri bir meslek yüksek okulunda kullanılmak üzere modellenmiş ve geliştirilen otomatik öğrenci devam sistemi üzerine bir çalışma yapılmıştır. Bu sistem yine aynı şekilde, katılım sürecini hızlandırması ve değerli eğitim zamanlarından tasarruf etmemizi sağlamaktadır. Ek olarak, bu sistem kullanılarak bir sınavda, öğrencilerin oturma düzeni öğretmenler tarafından ayarlanabilir (Hendry ve diğerleri, 2017: 1). Ayrıca eğitim alanında çevrimiçi ve çevrimdışı anket, ses dosyası ve çalışma kağıtlarına ipuçları yerleştirilmesi örnekleri verilmiştir (Çataloğlu ve Ateşkan, 2014: 10-13).

Mobil öğrenme adı altında eğitim alanında kullanılan QR Kodlar, öğrencinin konuya olan ilgi ve motivasyonunun ve öğrenme başarısının arttığını göstermektedir. Mobil cihazlar, öğrencilere basılı öğrenme materyalindeki bilgi ile mobil cihaz üzerindeki bilgiyi birlikte kullanarak daha iyi öğrenme çıktısı elde etme olanağı sunmaktadır. Mobil cihazların kolay taşınabilir olması, basılı kaynaklar (Kitaplar, yazılı ders notları) ile web sayfalarındaki bilgilerden yararlanılarak öğrencilerin öğrenmesine olumlu katkılar sağlamaktadır (Bilici, 2015: 101-102).

Kablosuz ve güvenlik uygulamaları için QR Kodlu anten yapılmıştır (Numan-Al-Mobin ve diğerleri, 2013: 1). QR Kodun kendisi herhangi bir metine, URL'ye ve alfasayısal içeriğe dayalı belirli bir kodu temsil etmektedir. Antenin 2,43 GHz'de 8,5 dB dönüş kaybı ve iyi bir alıcıyı temsil eden 1,25 dBi kazanç özelliği bulunmaktadır. Bu antenler, ek bir güvenlik özelliği ve / veya RFID etiket anteni (radyo frekanslı tanımlama) yerine kullanılabilmektedir (Numan-Al-Mobin vd., 2013: 1).

Otomobil hırsızlığı ve otomobil ile yapılan çeşitli suçlar giderek artmaktadır. Bunun için otomatik plaka tanıma sisteminde QR Kodlar kullanılmıştır. Bu sistem, araç kayıt plakalarını okumak için görüntülerde optik karakter tanıma (OCR) kullanan bir araç tarama tekniği olarak adlandırılabilir. Arabaları takip etmenin en iyi yolu kayıt numaralarıdır. Plaka tanıma sistemi bu gibi durumlar için en uygun çözüm olabilmektedir. Plakadaki sayıların ve harflerin okunmasındaki karşılaşılan hatalarda aracın tespit işlemi zorlaşmaktadır. Bu nedenle Otomobillere QR Kod eklenmesi önerilmektedir. Böylece daha hızlı yanıt alınabilmektedir. Görüntü işlemedeki sorunlar ortadan kalkmaktadır. Algılama tekniği ayarlanarak sorunlar giderilmektedir (Moharil ve Diğerleri, 2012: 5108).

Hammaddeden başlayarak nihai ürüne kadar her bir gıda ürününün dönüşüm aşamalarında verilerin izlenebilirliği ve ürün paketindeki temel verilerin basılması, tüketicilerin ürün kalitesine olan güvenini artırmaktadır. Her bir gıda ürünü için, ham ürün yetiştirme aşamasından başlayarak, gıda işleme, nakliye, depolama, perakende satış ve nihai tüketiciye ulaşmaya kadar verileri izlemek gerekmektedir. Temel verinin kullanıcıya (çoğunlukla son tüketici) öngörü kazanmasını sağlamak için, ürünün paketindeki verilerin ürünün yaşam döngüsünün kilit noktalarına hızlı bir şekilde QR Kodu şeklinde kaydedilmesini önermektedir. Önerilen sistemin verimli bir şekilde çalışması için, QR Kodunun üretim sırasında pakete uygun şekilde yerleştirilmesi ve ürün tüketicisi tarafından hızlı ve kolay veri okunması yoluyla hızlı ve güvenilir çalışmanın sağlanması çok önemlidir. Örnek olarak, meyveli yoğurtların veri takibi ve izlenmesi için kullanılmıştır.

İzlenebilirlik sistemi konsepti evrenseldir ve diğer ürünler içinde kullanılabilmektedir (Tarjan ve diğerleri, 2014: 1).

İş ekipmanlarında güvenlik takibi için QR Kod kullanılmaktadır. Sektörlere göre değişen iş ekipmanlarının güvenliğini sağlamak, iş kazalarının sayısını azaltmak ve sürdürülebilir güvenlik önemlerini sağlamak son derece önemlidir. Asma iskele, yük asansörü, vinç vb. tarzı makinalarına QR Kod çıktıları yerleştirilmiştir. Çalışanlara ve makinalara ait belgelere kolay ulaşım ve kullanım kolaylığı için yapılmıştır. Orijinal belgelere ulaşılabileceği gibi, çalışan personelin değişmesi gibi durumlarda linkin içeriği de ilave ekleme ve çıkartmalarla sürekli güncel tutulabilmektedir. Karekod içerisinde verilen link ile tüm çalışanların ve kontrollerin her daim istedikleri güncel bilgiye ulaşmaları sağlanabilmektedir. İş sağlığı ve güvenliğinde dokümantasyon kontrol ve takibi için "karekod barkodlama" sisteminin uygulanmasına ilişkin bir modelleme yapılmıştır. Bu modellemenin sonucu olarak karekod barkodlama uygulamasının iş sağlığı ve güvenliği hizmetleri içinde insan odaklı sistemleri ortadan kaldırarak, şeffaf anlaşılabilir ve sürdürülebilir bilgi bankaları oluşturabileceği iç denetim, dış denetim süreçlerini kolaylaştırabileceği gibi çıktılar elde edilmiştir (Elçi, 2014: 29-40).

Günümüzde kartvizitlerde, davetiyelerde, müzelerde de QR Kodlar yaygınlaşmaya başlamıştır. Kartvizite yerleştirilen QR Kod sayesinde, karekodun okutulduğu akıllı telefonun adres rehberine direk olarak kaydolabilmektedir. Ek olarak kişi veya firmalara ait bilgiler metin olarak da kodlanıp görüntülenebilmektedir. Davetiyelerde de benzer şekilde, karekodun içerisine düğün, toplantı, seminer vb. aktivitelerin salonuna ait genel bilgiler, lokasyon bilgileri, ulaşım ve iletişim bilgileri yer almaktadır. Bu sayede davet edilen yere, kişilerin kolay ulaşım amacı sağlanmaktadır (Bilici, 2015: 96-101). Almanya'nın Stuttgart şehrinde bulunan Mercedes-Benz müzesinde, etkinliklerin duyurulmasında, mobil olarak bilet satış hizmetinde ve dağıtımında, tarihi bölgelerde kullanılmıştır (Sanal, 2017: 34).

QR Kodların müzelerde kullanımı ile, tarihi eser hakkında detaylı bilgi vermek ve yeni neslin ilgisini çekmek amacı güdülmektedir. Bu kapsamda Türkiye'de hayata geçirilen uygulama ile Topkapı Sarayı, cep telefonlarıyla yurtdışına açılmıştır. İlk olarak Ayasofya Müzesi, Topkapı Sarayı Müzesi, Arkeoloji Müzeleri ve Kariye Müzesi'nde başlatılan uygulama özellikle yabancı turistlerden yoğun ilgi görmüştür. Seçilen kodun akıllı telefona okutulmasıyla birlikte, kullanıcın yönlendirildiği bilgi ekranından ilgili müze veya esere ait olarak Türkçe, İngilizce, Fransızca ve Almanca hazırlanmış olan açıklamalara ulaşılabilmektedir. Ayrıca Türkiye'deki diğer müzelerin adres, açılış ve kapanış saatleri ile giriş ücretlerine yönelik bilgiler de ekranlardan görülebilmektedir (Bilici, 2015: 98-99). Müze kullanımına bir diğer örnek olarak, çocukların dikkatini çekebilmesi amacıyla QR Kod kullanan çocuklar için müze mobil oyunu sunulmuştur. 11-14 yaş arası öğrenciler bir dizi bilmecelerle çözümlerini araştırmak için kişisel akıllı telefonlarını kullanmışlardır (Ceipidor ve diğerleri, 2009: 282-283).

Pazarlama endüstrisi, QR Kodları reklamcılığın tamamlayıcı bir yolu olarak kullanmaktadır. Bir reklamda, müşteriyi ürünle ilgili ek bilgilerin bulunduğu web sayfasına götürebilmektedir. 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 QR Kodu mobil telefonuna okutmalıdır. Daha sonra ürünü veya hizmeti satın almak için, ödeme sayfasına veya şirketin web sayfasına yönlendirilmektedir. En büyük ödeme şirketlerinden olan Paypal, bu ödeme yöntemini bazı ülkelerde kullanmaya başlamıştır (Kapsalis, 2013: 8).

QR Kod kullanımının şirketlere birçok yararı vardır. Şirkete veya markaya odaklanan tüketicilere anında daha fazla içerik sunmaktadırlar. QR Kod reklamcılığı, maliyetli olmayan bir yöntemdir. QR Kodun satış üretmeyi ve geliri arttırmayı başaran birçok örneği bulunmaktadır. Örneğin, Taco Bell (Meksika mutfağı usulü fastfood restoran), mevcut olan kutulardaki ve bardaktaki QR Kodlarını yazdırmak için MTV (müzik içeriği) ile birlikte çalışmaktadır. QR Kodun içeriği her hafta değişmektedir, bu nedenle bu kavram tüketiciler için hala yenidir ve tekrar ziyaretlerini teşvik etmektedir. Diğer bir örnek ise, Applebee bar restoranın sahibi, masalarda QR Kodlarını kullanmaya başlamıştır. QR Kod kullandıktan sonra satışlarında artış sağlamıştır. Ek olarak işletmeyi, işletmeye satan şirketler de QR kod kullanmaktadır. CRT Industrial Equipment Inc., yalnızca bir ekipmana 100.000 ABD Doları harcayan müşterilere hizmet vermek için QR Kodunu kullanmaktadır. Yukarıdaki örneklerin tümü, QR Kodun kullanılmasının özellikle şirket gelirleri olmak üzere şirketlere daha fazla avantaj getirebileceğini göstermektedir.

Sonuç olarak, şirketler QR Kodu kullanarak bütçeyi azaltabilmektedirler. Bilgi yayınlama ve marka paylaşımında reklam olmadan marka odaklı tanıtım için, bilgi paylaşımı sırasında uygun bir yol olarak kullanılabilmektedir (Qianyu, 2014: 44-47).

QR Kod Bankacılık dönemi ülkemizde ilk olarak Türkiye İş Bankası ile başlanmıştır. Patent başvurusunda bulunduğu "Parakod" uygulamasını hayata geçirmiştir (Türkiye İş Bankası A.Ş., 2012) Ardından QR Kod, ülkemizde diğer bankalar tarafından da kullanılmaya başlanmıştır. Kredi kartına ihtiyaç olmadan akıllı telefonlar ile ödeme yapılması mümkün olmuştur. Müşteriler, akıllı cihazlar ile internet ve mağazalarda hiçbir kart bilgisi girmeden ve kredi kartı bulundurmalarına gerek duymadan istedikleri ürün veya hizmeti QR Kod teknolojisi ile satın alabilmektedir. QR Kod ile para çekme veya yatırma işlemleri gerçekleştirilebilmektedir. Böylelikle bankacılık sektöründe QR Kod kullanımı artmaya başlamıştır (Öğütçü, 2019: 33-44).

1.3. QR Kodun Gelişimi ve Tarihçesi

QR Kod, 1994 yılında Japonya'da Denso Firması tarafından geliştirilmiştir iki boyutlu (2D) barkod türüdür. QR Kod açılımı "Quick Response" İngilizce çabuk tepki, hızlı yanıt veren anlamına gelmektedir. Karekod teknolojisi Toyota otomobil firmasının verimi arttırmak amacıyla, araç ve yedek parça üretimi ile imalatı sürecinde kullanılan parçaların etiketlenmesi ile ortaya çıkmıştır. Toyota patent haklarını 2010 yılında ücretsiz olarak açarak insanlığın kullanımına sunmuştur (Çataloğlu ve Ateşkan, 2014: 7).

Karekod genellikle kare motiflerden oluşmaktadır. Bu motif okuyucu cihazlar tarafından tarandığında, web sayfasına, elektronik posta adresine, iletişim bilgilerine, harita konumuna ulaşımı sağlamaktadır. Beyaz zemin üzerine siyah çubuk şeklinde oluşturulmuş temel kodlardan yani barkodlardan, ikinci nesil kare biçimindeki kodlara geçilmiştir. Belli bir algoritma ile oluşturulduğu için gerektiğinde değişiklik yapma imkânı sağlamaktadır. Karekodlar yazılı dokümanı ile sanal ortamı bütünleştirmektedir (Elçi, 2014: 11).

1.3.1. Barkod Nedir?

Barkod, değişik kalınlıktaki dik çizgi ve boşluklardan oluşan, verinin hatasız bir şekilde başka bir ortama aktarılmasında kullanılan bir yöntemdir (Taşkın, 2012: 4). Uluslararası standartlara sahip olan ve çeşitli kodlama biçimleri bulunan barkodlar, kodlanabilir bilgilerin barkod okuyucu cihazlar tarafından algılanarak, okunabilir hale getirilebilen simgelerdir. Diğer bir ifadeyle, yan yana dizilen ve farklı kalınlıkları bulunan siyah renkli çizgiler topluluğudur (Bayram ve Çetinkaya, 2007: 1). Çizgi kodu olarak da adlandırılırlar. Çizgi Barkodların bir örneği Şekil 1'de gösterilmektedir.

8 11204 01234 4

Şekil 1. Çizgi Barkod Örneği

Sayılar kümesinden oluşan çizgi barkodlar, barkod okuyucu cihazlar tarafından siyah ve beyaz çizgileri elektrik sinyallerine dönüştürülmektedir. Bu sinyaller okuyucu tarafından çözülerek anlaşılabilir rakam veya karakterlere çevrilmektedir. Çizgiler, ilgili objenin referans numarasını yani kodunu içermektedir. Bilgisayar ortamında obje ile ilgili olan bilgiler bu kodun karşılığına tanımlanmaktadır. Bu yüzden çizgi barkodun içerisine gömülmüş bir bilgi bulunmamaktadır (Arslan ve diğerleri, 2010: 394).

Ülkemizde son zamanlarda barkod ve Auto ED (Automatic Identification) oldukça yaygın olarak kullanılmaktadır. Otomatik tanımlama olarak karşımıza çıkan bu sistem, verilerin değişik yöntemler ile kimlik tanımlaması ve tanımlanan verilerin hatasız ve hızlı bir biçimde elektronik ortama aktarılmasını sağlamaktadır. Bu sistemler şu şekilde sıralanmaktadır;

- Barkod,
- MICR (Manyetik Mürekkeple Yazılmış Karakterlerin Tanınması),
- OCR (Optik Yöntemle Karakterlerin Tanınması),
- RF/ID (Radyo Dalgaları ile Tanıma),

- RF/DC (Radyo Dalgaları ile Veri İletişimi),
- Artificial Vision (Yapay Algılama),
- Voice Recognition (Ses ile Algılama),
- Sistem Entegrasyonu'dur.

Demiryolu sevkiyatındaki eşya ve araçların hızlı kontrolüne ihtiyaç duyulmasıyla birlikte barkod sistemine olan gereksinim doğmuştur. Barkod teknolojilerinin geçmişi 1950'li yıllara kadar dayanmaktadır. R&D demiryolu şirketi bu konuda ilk çalışmaları yapmıştır. Bu alanda ilk çözüm ise Sylviana isimli bir şirketten gelmiştir. Sylviana kuruluşunun ürettiği bu sistem, günümüzdeki optik yöntemlerle karakter tanıma teknolojisidir. 1968 yılında ise Computer Identics Corporotion Şirketi çalışmalar yaparak her türlü yüzeye basılabilmesini sağlamıştır. Tarihteki bu çalışmalar, günümüzde kullanılan modern barkod uygulamalarının temelini oluşturmuştur (Elçi, 2014: 3-4).

1.3.2. Barkod'un Tarihçesi

1940 yılında Amerika'da Draxel Teknoloji Enstitüsünde iki öğrenci tarafından geliştirilmeye başlanmıştır. 1949'da Norman Woodland ve Bernard Silver adındaki öğrenciler, hedef tahtasındakine benzeyen iç içe geçmiş halkalar şeklinde bir veri kodu için patent başvurusu yapmıştır. Ardından, tarayıcı prototipi yapılmıştır. İlk başlarda, kızılötesi ışığın altında parlayacak floresan mürekkeple oluşturulacak desenleri kullanmayı denemişlerdir. Fakat bu sistem çok maliyetliydi ve kullanışsızdı. Daha sonra N. Woodland, Mors kodu ilkesiyle çalışan ve tarayıcıya okutulabilecek bir etiket olması gerektiğini düşünmüştür. Fark olarak, noktalar yerine inceli kalınlı çizgiler kullanılmasıdır. Geliştirildikten sonra, o zamanlar IBM şirketinde çalışan Woodland 2 kez patent satın alma önerisinde bulundu ancak patent hakkını 1962'de Philco firması aldı ve sonra RCA firmasına satılmıştır. Daha sonra Woodland, Amerikalı George Laurer ile beraber Evrensel Ürün Kodu olarak bilinen ve 1973'te onaylanan 12 basamaklı karmaşık kodu geliştirmiştir. 26 Haziran 1974 günü sabah 08:01'de, Amerika'nın Ohio eyaletinde bulunan Troy Şehrindeki Marsh Süpermarket'in kasasında satın alınmakta olan bir paket sakız, Dünya'da barkod ile satılan ilk ürün olmuştur (Taşkın, 2012: 28).

1.3.3. Barkod'un Kullanım Alanları

Günlük hayatımızda en çok karşımıza çıkan barkod teknolojisi; süpermarketler, fabrikalar, satış otomasyonu, bagaj ve yolcu takibi, otoyollarda gibi alanlarda kullanılmaktadır. Süpermarketlerde, aldığımız her bir ürünün üzerinde bulunan barkodlar, çizgileri yardımıyla anabilgisayara fiyat ve stok bilgisini işleyebilmektedir. Ek olarak bu ürünlerin üzerinde bulunan OT/VT teknolojisi olan Radio Frequency Tag'leri sayesinde hırsızlıkların önüne geçilmektedir. Satış noktalarındaki elemanların barkod okuyucu vasıtasıyla satışı yapılan ürünü bilgisayara tanıtması ve yazıcıdan faturasını veya fişini basarak, ürünün veya hizmetin tahsilatının yapılmasını sağlamaktadır (Akyazı, 1994: 146).

Dik ve kalın çizgilerden oluşan doğrusal barkodlar en çok süpermarketlerde kullanılmaktadır. Ürünlerin üzerinde yer alan barkodlar sayesinde, optik okuyucular tarafından okunarak veri tabanına aktarılan bilgi ile ürünün fiyatına erişimi sağlamaktadır (Acartürk, 2012: 117).

Uluslararası standartlara sahip olan barkod, ince ve kalın çizgileri sayesinde, ürün adı, ürün fiyatı, firma adı, ürün kodu ve ürünün imal edildiği ülke gibi bilgiler içerebilmektedir. Ek olarak, kütüphane otomasyonu sistemi kurularak, kitapların kaydının bulunduğu veritabanı ile ilişkilendirilerek, kitapların hangi rafta veya bölümde olduklarını kolaylıkla bulunabilmesini sağlamaktadır (Bayram ve Çetinkaya, 2007: 1).

Fabrikalarda işçilerin mesai giriş ve çıkış saatlerinin kontrol edilmesi, izin kullanımları gibi zamanların değerlendirilip bunun sonucunda maaş ayarlamasının bilgisayar aracılığıyla yapılması barkod ile mümkündür. Bir yandan giriş ve çıkış yerlerinde barkod etiketlerinin kontrol edilmesi güvenlik bakımından da yardımcı olmaktadır. Taşıyıcı bantlar üzerinden geçen ürünler üzerindeki barkodların okunmasıyla birlikte stok kontrolü ve takibi sağlamaktadır (Akyazı, 1994: 146).

Ulaşım alanında, uçak biletlerine konacak barkodların okuyucular yardımıyla tanınması ve bagajları üzerine barkod etiketi yapıştırılması, bagaj ve yolcu takibini sağlamaktadır. Kara yolu ulaşımında ise, otoyollarda ve köprü geçişlerinde kullanılan araç üzerindeki etiketlerden otomatik olarak tanınmasıyla, yol ücreti araç sahibinin hesabından düşmektedir (Akyazı, 1994: 146).

1.3.4. Barkod Tipleri

Barkodlar bir boyutlu (1D) ve iki boyutlu (2D) olmak üzere iki türü vardır. Bir boyutlu barkodlar sadece rakam ve çizgilerden oluşurken, iki boyutlu barkodlar daha fazla karakter desteği ve daha çok veri depolanabilmesi, arşivlenebilmesini sağlanmıştır. İki boyutlu barkodlar, temel barkodların kullandıkları alana daha fazla bilgi sığdırma gereksiniminden doğmuştur. Bir boyutlu barkod 0 ve 1'lerden oluşur. Çizgileri değişken kalınlıklarda basılmaktadırlar. Baskı kalitesinin iyi olması, barkodu hatasız ve sağlıklı bir biçimde okunmasını sağlamaktadır. En çok tercih edilen okuma teknolojileri; lazer ve kamera teknolojileridir (Taşkın, 2012: 6-7).

Tek boyutlu barkodlara; EAN/UPC, code 39, codebar, code 128, PDF417, Postnet, Pharmacode gibi örnekler gösterilebilir. İki boyutluya göre daha az veri tutan tek boyutlu barkodlar, veritabanında bir kaydın anahtar değeri ya da bir ürünün uluslararası ürün anahtarı (Universal Product Key – UPC) değeri tutmaktadır (Taşkın, 2012: 8).

1.3.5. Barkod Çeşitleri

EAN/UPC (European Article Numbering / Uniform Products Code) toplu tüketim ürünleri içine konumlandırılan market ve eczanelerde kullanılan kod sistemidir. EAN/UPC kodu örneği Şekil 2'de gösterilmektedir. European Article Numbering, Avrupa'daki üreticilerin kullandığı bir barkod sistemidir. Uniform Products Code ise aynı sistemin Amerika'daki üreticiler tarafından kullanılan halidir (Akyazı, 1991: 147).

Şekil 2. EAN/UPC Barkodu Örneği

Interleaved 2/5: Çoğunlukla endüstriyel ortamlarda hareketi takip etmek istenilen ürünlere kimlik tanımlamakta kullanılmaktadır. Bu barkod çeşidi ile sadece nümerik olarak kodlama işlemi yapılabilmektedir. Interleaved 2/5 barkodu Şekil 3'te gösterilmektedir (Akyazı, 1991: 147).

Şekil 3. Interleaved 2/5 Barkodu Örneği

PDF 417: Daha güvenilir, gizli ve daha çok bilgi depolayabilen, küçük bir alana 2000 adet numerik ve alfa numerik karakterler kodlayabilen barkod çeşididir. Şekil 4'te PDF 417 barkodu gösterilmiştir (Elçi, 2014: 13-14).

Şekil 4. PDF 417 Barkodu Örneği

Her ülkenin kendine ait barkod numarası vardır. Türkiye'de üretilen ürünlere ait barkod numaraları "869" ile başlamaktadır. Türkiye'de üretilen ürünlere ait bir barkod örneği Şekil 5'te gösterilmiştir (Taşkın, 2012: 8-11).

8 69 000 06200

Şekil 5. Türkiye'de Üretilen Ürünlere Ait Bir Barkod Örneği

Code 39 (code 3 of 9): Hem numerik hem de alfanumerik karakterler kodlanabilen barkod çeşididir. Üretim hattında veya kütüphanelerde kitapların ve üyelerin kodlanmasında kullanılabilir (Akyazı, 1991: 147).

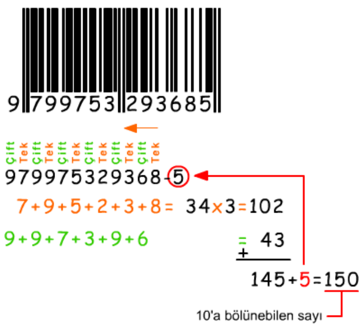
CodeBar: Çoğunlukla sağlık sektöründe kullanılır. Numerik karakterler kodlanabilen barkod çeşididir (Akyazı, 1991: 147).

Code128: Endüstriyel ortamlarda kullanılan numerik ve alfanumerik karakterler ile kodlanabilen barkod çeşididir (Akyazı, 1991: 147).

Ülke kodundan sonra gelen kodlar ise sırasıyla; firma kodu, ürün kodu ve kontrol kodudur. Firma kodu, Türkiye Odalar ve Borsalar Birliği'ndeki (TOBB) Mal Numaralandırma Merkezinden, firmalar tarafından talep edilmektedir. Ürün kodu, ise ürüne verilen yani diğer ürünler ile ayırt edilmesini sağlayan koddur. Kontrol kodu ise hatalı okuma ihtimaline karşı konulmuştur. Barkodda bulunun bu kısımlar Şekil 6'da gösterilmiştir (Taşkın, 2012: 8-11).

Şekil 6. Barkodda Bulunan Alanlar

Barkodda bulunan kontrol mekanizması, Sağdan başlamak üzere barkoddaki sayıları tek ve çift diye ayırmaktadır. Burada ilk hane tek sayılır, ikinci hane ise çift sayılmaktadır. Tek olarak ayrılan sayılar toplanarak sonuç 3 ile çarpılmaktadır. Çift olarak işaretletmiş sayılar ise toplanmaktadır. Elde edilen bu sayılardan her iki sayı da toplanmalıdır. Çıkan sonuca 10 sayısının katı olacak şekilde bu toplama eklenmesi gereken sayı bulunmaktadır. Eklenecek olan sayı ile kontrol sayısı birbirine eşit yani aynı sayı ise okuma işlemi hatasız kabul edilmektedir. Yapılan bütün bu işlemlere örnek olarak hata kontrol işlemi Şekil 7 de gösterilmiştir (Taşkın, 2012: 8-11).



Şekil 7. Hata Kontrol İşlemi

Amerika posta servisi firması UPS tarafından kullanılan barkod Maksi Kod iki boyutlu barkoddur. Fazla veri temsil edebilmektedir. Görünüm olarak QR Koda benzemektedir.

Şekil 8. Maksi Kod İki Boyutlu Barkod Örneği

İki boyutlu barkod olan QR Kodun değişik versiyonları mevcuttur. Bu konuya 1.4 QR Kodun yapısında devam edilecektir.

1.4. QR Kodun Yapısı

QR Kod ile depolanan ve 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

QR Kodda saklanabilecek veri miktarı, moduna, versiyonuna ve hata düzelme seviyesine göre değişiklik göstermektedir. QR Kodun 1.versiyondan başlayarak (1,2,3, ..., 40) 40 farklı versiyonu vardır (Kieseberg Ve diğerleri, 2010: 2).

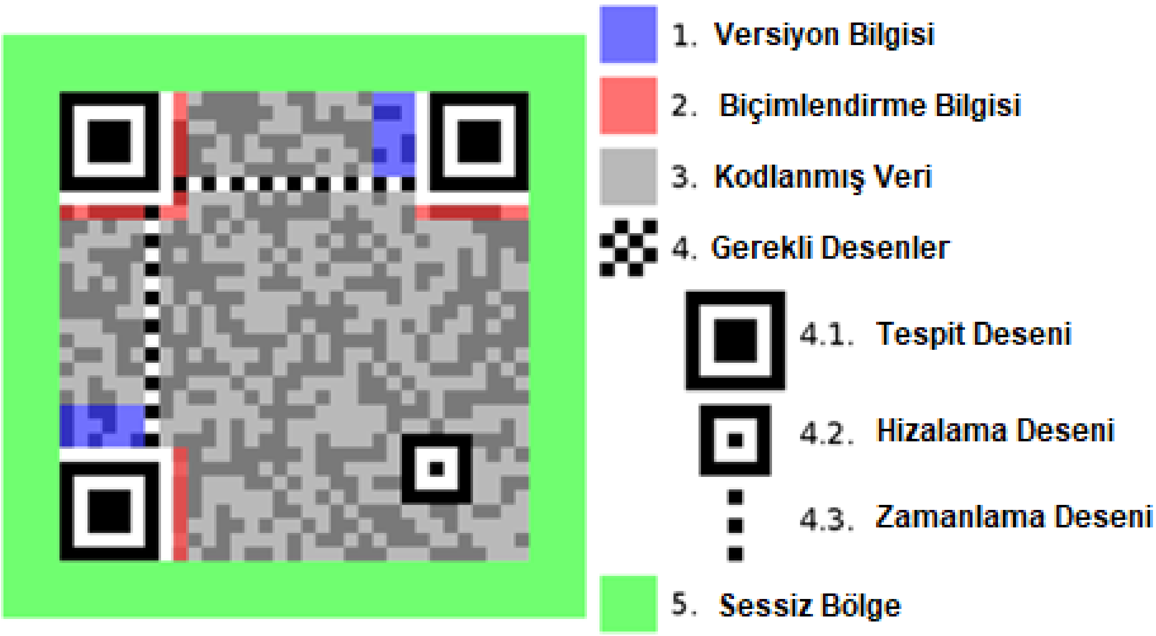
Tablo 1'deki QR Kodlar taratıldığında "ABC123" metnini içeren farklı QR Kod versiyon örnekleri verilmiştir.

Tablo 1. QR Kodun farklı versiyonları (1,5,10,20,30 ve 40.versiyon örnekleri) (Sharma, 2012: 1).

Versiyon 1	Versiyon 5
Versiyon 10	Versiyon 20
Versiyon 30	Versiyon 40

QR Kod hata düzeltme yeteneğine sahiptir. Kirli veya kısmen hasarlı olsa bile okunabilir. Hata düzeltme seviyesi ise; Düşük (%7), Orta (%15), Kalite (%25), Yüksek (%30) şeklindedir (Sharma, 2012: 1).

Şekil 9'da QR Kodun yapısı gösterilmiştir. Devamında ise QR Kodun yapısı ile ilgili özellikleri anlatılmaktadır.



Şekil 9. QR Kod Yapısı (Polat, 2014: 3).

1. Versiyon Bilgisi (Version Information): 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 (Format Information): Biçimleme Bilgisi bölümü, ayırıcıların yanındaki 15 bitten oluşur ve QR Kodun hata düzeltme seviyesi ve seçilen maskeleme modeli hakkında bilgiyi içermektedir.

3. Kodlanmış Veri (Encoded Data): QR Kodun verileri bu alanda depolanır. Veriler, '0' ve '1' binary numaralarının siyah ve beyaz hücrelere çevrilmesiyle saklanmaktadır.

4. Gerekli Desenler (Required Pattern):

4.1. Tespit Deseni (Finder Pattern): QR Kodun tüm köşelerinde, sadece sağ alt köşesi hariç olmak üzere üç aynı kareden oluşmaktadır. Her desen 3x3'lük matrise dayanmaktadır. Bu kısım, okuyucu yazılımın QR Kodunu tanımasını ve doğru yönlendirmesini sağlamaktadır. Bir piksel genişliğe sahip beyaz **Ayırıcılar (Seperators)**

ile çevrelenerek tanınmasını ve gerçek verilerden kolaylıkla ayrıt edilmesini kolaylaştırılmıştır. Bu şekillerde yapılan herhangi bir değişiklik kod çözücülerin kodu okumasını engelleyebilir.

4.2. Hizalama Deseni (Aligment patterns): Bu desen, QR okuyucunun kod büküldüğünde veya kavislendiğinde bozulmamasını ve düzeltmesini sağlamaktadır. Orta derecede görüntü bozulmalarını engellemek için çözücü yazılımını desteklemektedir. QR Kod versiyon 1'de hizalama kalıplarına sahip değilken versiyon 2'de QR Koda boyutu ile birlikte daha fazla hizalama deseni eklenmiştir.

4.3. Zamanlama Deseni (Timing Pattern): 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 ve Jamankar, 2013: 176).

5. Sessiz Bölge (Quiet Zone): QR Kodun çevresindeki verinin olmadığı boş alandır. Bu alana hiçbir şey yazılamamakta ve basılamamaktadır. En az 4 modül (her nokta 1 modüldür) genişliğinde olmalıdır. Bu boş alan sayesinde kod, hatasız bir biçimde okunmaktadır (Polat, 2014: 3).

1.5. QR Kod Tipleri

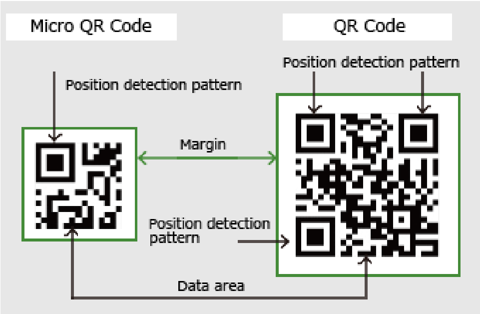
a. Versiyon 1 ve Versiyon 2

Versiyon 1: QR Kodu, 1.167 rakamı kodlayabilen ve maksimum sürümü 14 (73 x 73 modül) olan bir koddur.

Versiyon 2: Model 1'i geliştirerek oluşturulan QR Kodu, bu kod bir şekilde bozulsa bile sorunsuz okunabilmesini sağlamaktadır. Kavisli bir yüzeye yazdırılan veya okuma görüntüleri nedeniyle okuma görüntüleri bozuk olan QR Kodları, içine gömülmüş bir hizalama düzenine bakarak verimli bir şekilde okunabilmektedir. Maksimum versiyon 40'tır. (177 x 177 modül) olan 7.089 rakamı kodlayabilmektedir (Denso Wave Incorporated, 2013).

b. Mikro QR Kod (Mini)

Mikro QR Kod, Daha küçük bir alana yazdırılabilmesi için yalnızca bir yön algılama desen kodudur. Micro QR Kodunun önemli bir özelliği, belirli bir alan gerektiren normal QR Koduna kıyasla yalnızca bir konum algılama düzenine sahip olmasıdır, çünkü konum algılama düzenleri bir sembolün üç köşesinde bulunmaktadır. Ayrıca, QR Kod, bir sembolün etrafında en az dört modül genişliğinde bir kenar boşluğu gerektirirken, Micro QR Kod için iki modül genişliğinde bir kenar boşluğu yeterlidir. Micro QR Kodunun bu yapılandırması, QR Kodundan daha küçük alanlara yazdırmanıza izin vermektedir. Şekil 10'da Mikro QR Kod örneği verilmiştir (Tiwari, 2016: 43).



Şekil 10. Micro QR Kod Örneği

c. iQR Kod:

iQR Kodu konumunun ve boyutunun kolayca okunmasını sağlayan bir matris tipi 2D koddur. Bu kod, geleneksel QR Kodundan ve Mikro QR Kodundan daha küçük olanlardan bunlardan daha fazla veri depolayabilen büyük kodlara kadar geniş bir kod yelpazesine izin vermektedir. Bu kod, çeşitli alanlarda geniş bir uygulama yelpazesine olanak tanıyan dikdörtgen kod, siyah beyaz ters çevirme kodu veya nokta desen kodu (doğrudan parça işaretleme) olarak da yazdırılabilir ve çeşitli alanlarda geniş bir uygulama yelpazesi bırakmaktadır. Şekil 11'de iQR Kod örneği verilmiştir (Tiwari, 2016: 43).

Şekil 11. iQR Kod Örneği

d. SQRC Kod: A Single QR Code

Tek bir QR Kodu genel verileri ve özel verileri taşıyabilmektedir. Özel veriler, yalnızca veri koruması sağlayan şifreleme anahtarına sahip özel bir okuyucu ile okunabilmektedir. SQRC normal QR Koduyla tamamen aynı olduğu için sahteciliği ve kurcalamayı önleyebilmektedir. Normal QR Koddan farkı güvenli olmasıdır. Bilgiyi bir şifreleme anahtarıyla gizleyerek gizli tutmak ve bilgileri okuyabilen cihaz türlerini kısıtlamak, böylece yalnızca belirli kişilerin okuyabilmesi mümkündür (Denso Wave Incorporated, 2013).

e. Çerçeve (Frame) QR Kod

Bu kodda, görüntüyü tutmak için bir alan veya çerçeve bulunmaktadır. Çerçevenin şekli ve rengi esnek bir şekilde değiştirilebildiği için, kod çeşitli uygulamalara sahiptir. QR Koda resim entegre edilebilmektedir. İnsanlar tarafından daha dikkat çekici olmaktadır. Yalnızca siyah beyaz olan QR Koda göre, resim olduğu için çıplak gözle ne olduğu hakkında bir fikir sahibi olunabilmektedir (Denso Wave Incorporated, 2013). Şekil 12'de Çerçeve QR Kod örneği verilmiştir.

Şekil 12. Çerçeve (Frame) QR Kod Örneği

1.6. QR Kod Oluşturma

Şahsi veya ticari amaçlı kullanılabilen QR Kodların oluşturulması için çeşitli yöntemler: bilgisayarınıza indirebileceğiniz QR Kod oluşturan program (örnek: My QR Code Generator) veya çeşitli online web siteleri bulunmaktadır (Çataloğlu ve Ateşkan, 2014: 7).

Bu yöntemlerle hazır tema ve logo ile kodu renkli ve değişik şekillerde oluşturabilmek mümkündür. Ayrıca, QR Kodu oluştururken eklediğiniz URL yerine size farklı ve daha kısa bir URL tanımlayabilmektedirler.

II. BÖLÜM: QR KOD SALDIRILARI

QR Kodlar hem insan etkileşimine hem de otomatik sistemlere saldırmak için kullanılabilmektedir. Çalışmanın ikinci bölümünde güveliğin önemi, düzenlenebilecek saldırılar, üçüncü bölümünde ise bu saldırılara karşı alınabilecek önlemlere yer verilmiştir.

QR Kodu, kolay üretilişi ve dağıtımı, geniş depolama kapasitesi ve hızlı okunabilirliği nedeniyle popüler olmuştur. QR Kodları kullanıcıları daha fazla bilgi veya hizmet sağlayabilecek ilgi alanlarına yönlendiren web sitelerine yönlendirmek için kullanılabilmektedir. Bununla birlikte, bir QR Kodunu tarayarak, kullanıcılar kolayca bir kimlik avı web sitesi (phishing) veya bir kötü amaçlı yazılım dağıtıcı gibi zararlı bir web sitesine yönlendirilebilir. Bunun nedeni, kullanıcıların QR Kodunda kodlanan bilgileri taramadan önce bilmemeleridir. Bu nedenle, saldırganlar bundan yararlanabilir ve çeşitli saldırı türleri için QR Kodlarını kullanabilmektedir (Shin ve Yao, 2013: 49).

2.1. Phishing (Kimlik Avı)

Sosyal mühendislik, yetkisiz olarak insanların gizli bilgilerine ulaşabilmek için manipüle etme sanatıdır (Mitnick ve Simon, 2013). Bilgileri çalmak veya birinin erişmeye yetkili olmadığı bir sisteme zorla giriş yapmak için kullanılmaktadır. 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 (Kapsalis, 2013: 9-10). 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: 9-10). Yapılan bir araştırmada QR Kodlarını içeren posterleri, kimlik avı için 139 farklı yere dağıtıldığında dört hafta boyunca, web sitelerini 225 kişinin ziyaret ettiği görülmüştür. QR Kodu tarayanların, %85'inin ilgili URL'yi ziyaret ettiğini gözlemlenmiştir. Yapılan ankete göre, merakın QR Kodlarını taramak için en büyük motive edici faktör olduğunu göstermektedir. Kullanıcıların %75'lik kısmı, QR Kodunu meraktan veya eğlence için taramışlardır. Geri kalan kısmı ise, daha fazla bilgi almak için taramışlardır (Vidas ve diğerleri, 2013: 1-15).

QR Kodları, reklamlarda, hedef kitleyi özel tekliflere veya belirli ürünler hakkında ek bilgilere yönlendirmek için kullanmaktadır. Saldırgan, QR Kodlarının yerini alabilir ve kullanıcı taradığında, bilmeden sahte bir sayfaya yönlendirilebilir (Sharma, 2012: 5). Saldırgan, kod okunduğunda **kötü amaçlı yazılımın (Malware)** otomatik olarak indirileceği bir sayfaya yönlendirilecek şekilde QR Kodunda bir URL kodlayabilmektedir. Saldırgan, bu şekilde **virüs, casus yazılım, Truva atı** veya kullanıcıya ve sisteme büyük zararlar veren **solucanlar** içeren yazılımın yayılımını gerçekleştirebilmektedir.

Yeni sosyal mühendislik saldırısı vektörü olan QRLJacking (QR Code Login Jacking), hesaplara giriş yapmanın güvenli bir yolu olarak "QR Koduyla giriş yap" özelliğini kullanan tüm uygulamaları etkileyebilecek, oturumu ele geçirme yeteneğine sahip basit bir sosyal mühendislik saldırı vektörüdür (Github, 2019). Özetle, mağdur, saldırganın QR Kodunu tarayarak oturumun ele geçirilmesine neden olmaktadır (Owasp, 2019).

2.2. SQL ve Komut Enjeksiyonu

SQL ve Komut Enjeksiyonu, otomatik sistemlere kolaylıkla, bilgisayar korsanları tarafından enjekte edilebilmektedir. QR Kod çözme yazılımının, bir veri tabanına bağlandığı ve arka veri tabanında 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 çalıştırabilmekte ve bu bilgilerin başka türlü yetkili bir kullanıcı için tasarlanan potansiyel bir bilgisayar korsanına gösterilmesine yol açabilmektedir. Bununla birlikte, QR Kodları henüz veri tabanı sorgulamaları sağlamak için kullanılmamıştır. Ancak gelecekte böyle bir durumda, QR Kodları bu tür sistemlere saldırmak için kullanılabilmektedir. Google, Google hesabına girişleri için QR Kodunu kullanma denemeleri yapılmıştır (Sharma, 2012: 4).

Komut enjeksiyonu yönteminde ise saldırgan, sayfadaki içeriği değiştiren bir HTML kodu enjekte edebilmektedir. Kullanıcı değiştirilen sayfayı ziyaret ettiği zaman, web tarayıcı kodu yorumlamakta ve bu da kullanıcının QR Kod okuttuğu cihazında (çoğunlukla akıllı telefon veya tablet) kötü amaçlı komutların yürütülmesine neden olmaktadır (Ahuja, 2014: 3879). 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 yararlanabilmektedir. Bu şekilde bir saldırgan rootkit, spywares, Servis Engelleme (DoS) saldırısı başlatabilir veya uzaktaki bir bilgisayara bağlanabilmekte ve oradan sistemin kaynaklarına erişebilmektedir (Sharma, 2012: 5).

Okuyucu yazılımının bilgisayarlarda veya akıllı telefonlarda farklı uygulamaları, komut enjeksiyonunun temizlenmemesi durumunda, komut enjeksiyonu veya geleneksel arabellek aşımı (buffer overflows) yoluyla saldırıya uğrayabilmektedir. Saldırgan, kullanıcının iletişim bilgileri veya e-posta, SMS gibi iletişim içeriği de dahil olmak üzere tüm akıllı telefon üzerinde kontrol sahibi olabilmektedir (Kieseberg ve diğerleri, 2010: 6).

2.3. Tarayıcı Tabanlı Saldırıları ve Siteler Arası Komut Dosyası Çalıştırma

Tarayıcı tabanlı saldırıları ve siteler arası komut dosyası çalıştırma saldırılarını (XSS/Cross Site Scripting) yürütmek için bir QR Kodu kullanılabilmektedir. Bir QR Kodu şifreli URL içerebilmektedir. 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 (Sharma, 2012: 4-5).

Kötü niyetli komut dosyalarının, iyi huylu ve güvenilir web sitelerine enjekte edildiği bir enjeksiyon türü olan XSS saldırıları, saldırgan tarafından, genellikle bir tarayıcı tarafı komut dosyası biçimindeki kötü amaçlı kodu farklı bir son kullanıcıya göndermek için bir web uygulaması kullandığında ortaya çıkmaktadır. Bu saldırıların başarılı olmasına izin veren kusurlar oldukça yaygındır. Bir web uygulamasının, oluşturduğu çıktı içindeki bir kullanıcıdan gelen ve doğrulamadan veya kodlamadan girdi kullandığı her yerde ortaya çıkmaktadır. Saldırgan, bir kullanıcıya kötü amaçlı bir komut dosyası göndermek için XSS kullanabilmektedir. Kullanıcının tarayıcısının, betiğin güvenilmemesi gerektiğini bilmesi mümkün değildir ve komut dosyasını yürütmektedir. Komut dosyasının güvenilir bir kaynaktan geldiğini düşündüğünden, kötü amaçlı komut dosyası, tarayıcı tarafından tutulan ve bu sitede kullanılan tüm çerezlere, oturum simgelerine veya diğer hassas bilgilere erişebilmektedir. Bu komut dosyaları bile HTML sayfasının içeriğini yeniden yazabilmektedir (Li ve diğerleri, 2018: 241-255).

2.4. Dolandırıcılık / Sahtekarlık (Fraud)

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 kullanılabilmektedir (Kieseberg ve diğerleri, 2010: 5). 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 yapabilmekte veya kullanıcı adına kredi çekebilmektedir (Koygun, 2018). 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. İki farklı saldırı yöntemi mevcuttur. Bunlardan ilki her iki rengin de değiştirilmesidir. Saldırgan herhangi bir modülü ters çevirerek, siyahtan beyaza veya beyazdan siyaha olarak değiştirebilmektedir. Tek renk değişiminde ise saldırgan, tek bir rengi değiştirebilmektedir. Beyaz modülleri yalnızca siyah olarak çevirebilmektedir. Sadece bir kalem kullanarak anında tek bir posteri değiştirebilmektedir.

2.5. Gerçekleştirilen Saldırılar

2011 Eylül ayında, Kaspersky Lab tarafından kötü niyetli bir QR Kod tespit edilmiştir. Bu saldırı yöntemi, kullanıcı tarafından QR Kod taratıldığı zaman bir web sitesine yönlendirmekte ve kullanıcının haberi olmadan cihazına zararlı bir dosya indirilmektedir. Aynı zamanda mobil uygulamalar için QR Kodları içeren birçok kötü amaçlı web sitesi, numaralara kısa mesaj gönderebilen Truva atı (trojan) tespit edilmiştir (Wane ve Jamankar, 2013: 178).

Sosyal medya hesabında çıkan sahte banka reklamlarında, linke tıklayıp çekilişe katılma hakkı kazanın, linkten mobil şubeye giriş yaparsanız ikramiye veya ödül kazanacaksınız gibi söylemlerle kullanıcıları kandırmaktadırlar. Kullanıcı linke tıkladıktan sonra dolandırıcının ekranına düşmekte ve yasal kullanıcının girdiği bilgiler ile dolandırıcı tarafından bankada işlem yapılabilmektedir. Banka, kullanıcıya güvenlik için bir şifre gönderdiğinde kullanıcı o şifreyi sahte web sitesi üzerinden sisteme girdiği için şifre kötü niyetli kişilerin eline geçmektedir. Kötü niyetli kişiler kişisel bilgi ve şifreye ulaştığı için, o şifre ile QR Kodunu ele geçirip istediği ATM'den kullanıcı kartı olmadan işlem yaparken yasal kullanıcı ise bütün bu süreçte sadece hata mesajı almaktadır.

Çin'de ise, dolandırıcılığı önleme amaçlı QR Kod Ödemeleri durdurma karar alınmıştır. Çin Halk Cumhuriyeti Merkez Bankası'nın yaptığı açıklamalara göre, QR-kod ödeme sistemi bir süredir Çin içerisinde kara para aklamak ve dolandırıcılık gibi sebeplerle kullanılmaktadır. Özellikle de bu ödeme yöntemini insanlara sağlayan Alibaba ve Tencent'e bir süredir bu konuda başvurular yapılmasına rağmen, durumun önü alınamamaktadır. Bu sebeple Çin Halk Cumhuriyeti Merkez Bankası, QR-Kod aracılığıyla yapılan ödemeleri durdurma kararı almıştır (Erdal, 2018).

2012 yılında ülkemizde İzmir, Atatürk Stadyumu'nda Karşıyaka ve Göztepe arasında oynanan maçta, tribünde Karşıyakalı taraftarlar tarafından hazırlanan QR Kod içeren bir pankart açılmıştır. Göztepe taraftarları tarafından 3G akıllı cihazlarla okutulan pankartta, Göztepe'ye karşı çeşitli dillerde yazılan küfür ve argo sözcükler içermektedir. Maçı kaybeden Karşıyaka taraftarlarının açtığı bu pankart sadece ülkemizde değil, Dünya spor basınının da dikkatini çekmiştir. Polis güvenlik kameraları fotoğraflar yardımıyla, pankartı hazırlayıp açan kişilerin tespiti ve haklarında işlem yapılması için çalışma başlatmıştır (Milliyet Gazetecilik ve Yayıncılık A.Ş., 2012).

Şekil 13. Milliyet Gazetecilik ve Yayıncılık A.Ş., 2012, Tribünde QR Kod pankartı

2016 yılında, Garnizon Bilgi Güvenliği Ltd. Şti., Berk Göksel ve Alper Başaran tarafından "QR-Code'daki olta Bir farkındalık deneyi ve QR Kodların sosyal mühendislik saldırılarında kullanılması" araştırması yapılmıştır. Hazırlanan zararsız QR Kod afişlerini Türkiye'nin çeşitli illerinde, üniversite ve sokaklara asılmıştır. Kullanıcılar tarafından okutulan QR Kodlar, bir bilgilendirme sayfasına yönlendirilmiş ve bu sayede istatistiki bilgilere ulaşmışlardır. Çalışma toplamda yaklaşık 3 ay sürmüştür. QR Kod afişlerini yönlendirdikleri sayfada bilgilendirme mesajı olarak "Oltalandınız ! Ama paniklemeyin..

Burada kötü niyetli kimse yok.” bilgisi verilmiştir. Bu mesaj ekranı Şekil 14’te verilmiştir (Göksel ve Başaran, 2016).

Şekil 14. QR Kodlardaki Tehlike Araştırmasının Phishing için Hazırlanan QR Kodun Yönlendirdiği Bilgi Mesajı

Garnizon Bilgi Güveliği şirketi tarafından, Başkent Ankara, Ayrancı Mesnevi Sokak ile popüler olan Tunalı Hilmi Caddesine ve Bilkent Üniversitesi Kampüsüne QR Kod afişleri asılmıştır. Ek olarak, İstanbul Taksim Meydanı ile ODTÜ Kıbrıs Kampüsü’ne de QR Kod afişleri asılmıştır. QR Kod okutan cihazlara bakıldığında, tüm çalışma dahil Android işletim sisteminin %44,7’lik oranla yüksek olduğu, ancak sadece Bilkent Üniversitesi’nde %66,7’lik oranla IOS’un yüksek olduğu görülmüştür. Ankara 3854 kişi, İstanbul 5101 ve Kıbrıs 72 kişi olmak üzere toplam kurban sayısı 9027 kişidir (Göksel ve Başaran, 2016). Eğer yapılan araştırma için düzenlenen phishing saldırısı zararsız olmasaydı, 9027 kişi bu saldırıdan etkilenecekti.

III. BÖLÜM: QR KOD SALDIRILARINA KARŞI ALINABİLECEK ÖNLEMLER

İkinci 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 gerekmektedir. QR Kodlar insanlar tarafından okunamadığı için, kullanıcıya bilgi vermek için içerik gösterimi yapılabilir (Krombholz ve diğerleri, 2014: 8). Bunun yanı sıra QR Kod okutmak için özel olarak geliştirilmiş güvenli QR Kod okuyucuları kullanarak okutulan QR Kodun Güvenilirliği test edilebilir.

QR Kodlarıyla ilgili çeşitli güvenlik sorunlarının ele alınması için yaklaşımlar vardır. Kullanıcı belirli bir bağlantıyı açmadan önce URL'yi manuel olarak kontrol etmelidir. Ayrıca, bir web sitesinin geçerli bir sertifikası yoksa veya güvenli olmayan bir bağlantı kurmaya çalışırsa, QR Kod okuyucusu kullanıcıyı uyarmalıdır. Dijital imzalar QR Kodunun içine dahil edilebilir. Ayrıca QR Kodlarını kullanarak eşzamanlı şifreleme ve verilerin gizliliği sağlanabilmektedir (Ahuja, 2014: 3879).

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 ve diğerleri, 2014: 2).

(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 standardizasyonuna ve entegrasyonuna 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 gerekmektedir (Krombholz ve diğerleri, 2014: 7-8). 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 (David Ulevitch, 2006) gibi halka açık kara listesinden daha iyi ve algılama mekanizması %82,9 daha fazla URL saptama yeteneğine sahip olduğu bilinmektedir (Alnajjar ve diğerleri, 2016: 553-560).

(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 geçilebilmektedir. 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 izlemektedir. Bu desen, dikkate alınan modülün renginin değiştirilip değiştirilmeyeceğini belirtmek için kullanılan maske tarafından belirlenmektedir. 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 ve diğerleri, 2014: 8).

Saldırılar kısmında bahsedilen QRLJacking'e karşı alınabilecek önlemler arasında, en basit korunma yöntemi QR Kod ile giriş yapılmamasıdır. Diğer önlemler ise; oturum onayı istenmesi, yani oturum açılırken bir onay mesajı ya da bildirimi gelmesi olacaktır. IP kısıtlamaları, Farklı ağlarda (WAN) herhangi bir kimlik doğrulama işlemini kısıtlamak, saldırıları en aza indirecektir. Lokasyon Bazlı Kısıtlamalar yapılabilmekte, yani farklı lokasyonlara dayalı kimlik doğrulama işlemlerinin kısıtlanması sağlanabilmektedir. Ses Tabanlı Kimlik Doğrulama, bu tür saldırıları hafifletme tekniklerinden birisidir. Ses temelli kimlik doğrulama adımını bu süreçte, eşsiz veri üretmenin ve orijinal formuna (SlickLogin ve Sound-Proof) geri dönebilecek sese dönüştürmenin mümkün olduğu bu tür bir teknoloji vardır. Bu yüzden bu teknoloji ile QRLJacking'e karşı önlemler alınabilmektedir (Owasp, 2019).

3.1. Maskeleme Yöntemi

Maskeler, siyah ve beyaz modülleri iyi bir şekilde dağıtarak yeni bir QR Kod oluşturmak için kullanılmaktadır. 50:50 oranına yakın olarak tüm kodun üzerine dağıtılmaktadır. Bu, resmin kontrastını arttırır ve böylece cihazların onu çözmesine yardımcı olmaktadır. Bir QR Kod oluşturulurken QR Kodun her bir bölümüne (Şekil 9) maske uygulanabilmektedir. Çıkan sonuçlar derecelendirilmektedir. Derecelendirmeye göre en iyi dağılımla sonuçlanan maske seçilmektedir (Kieseberg vd., 2010: 3).

Teknik özelliklere uygun bir QR Kodunda siyah beyaz modüllerin dağılımı, belirli bir modeli izlemektedir. Bu desen, dikkate alınan modülün renginin değiştirilip değiştirilmeyeceğini belirtmek için kullanılan maske tarafından belirlenmektedir. Hata düzeltici Reed-Solomon kodlarının sağladığı sağlamlık nedeniyle, belirli derecede bozuk piksellerin QR Kodunu çözme üzerinde olumsuz bir etkisi yoktur. Siyah ve beyaz modüllerin eşit dağılımından sapma ne kadar yüksekse, QR Kodunun değiştirilme olasılığı o kadar yüksektir. Okuyucu yazılımını güvenceye almak ve maskeleme özelliklerini kullanmak için hata oranı ile güvenlik arasındaki değişimin ayrıntılı bir analizi faydalı olacaktır (Krombholz vd., 2014: 8).

3.2. Filigranlama

İnternet ve medyadaki ticari faaliyetlerin çoğalması nedeniyle güvenliği arttırmak gerekmektedir. Zhang ve Yoshino çalışmalarında; QR Kodların içine dijital görüntüler yerleştirmek için yeni bir filigran basma yöntemi geliştirilmiştir. Bu yöntem, kesikli dalga dönüşümü (Discrete Wavelet Transform-DWT) üzerine kuruludur. DWT tabanlı filigran kullanılarak, orijinal görüntü bloklara ayrılıp, filigran sinyalleri içine gömülmektedir. JPEG sıkıştırma için sağlam olduğunu göstermişlerdir. Gömülü bilgiler, görüntüler içeriğe göre orijinalin %11'ine kadar sıkıştırılsa bile doğru şekilde çıkarılabilmektedir (Zhang ve Yoshino, 2008: 3-6). Kötü niyetli kişiler tarafından artan saldırılar nedeniyle, dijital filigranlı QR Kodlar güvenlik alanında dikkat çekmektedir. QR Kodu DWT-Genetik Algoritmaya dayanan bir ses filigranı şeması ile filigranlama üzerine çalışmalar yapılmıştır. Böylece, veri gizleme için yeni bir yöntem önerilmiştir (Poomvichid vd., 2012: 171-174).

3.3. Dijital İmza

Güvenliği arttırmak için etkili bir araç olduğu kanıtlanmıştır. Kodun yaratıcısını doğrulamak ve böylece QR Kodunun değiştirilip değiştirilmediğini kontrol etmek için dijital imzaların QR Kod standardizasyonuna ve entegrasyonuna önem verilmelidir. 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 azaltmaktadır. Ayrıca, QR Kod okuyucularının dijital imzaları doğrulayacak ve SSL'ye benzer şekilde doğrulamanın başarılı olup olmadığını belirtecek şekilde uyarlanması gerekmektedir. Sonuç olarak, dijital imzaların QR Kod ile entegrasyonunu geliştirilmelidir (Krombholz ve diğerleri., 2014: 7-8).

Akıllı cihazlar, tablet gibi ürünlerde yüklü bir güvenlik yazılımı bulunmamaktadır. Ek olarak, bir güvenlik yazılımının yüklü olması da saldırılara karşı koruma sağlayacaktır.

Bu tip güvenlik programlarını yüklemek, siber suçluların kötü niyetli saldırılarına karşı daha duyarlı olmaktadır. Bunun için, uygulama mağazasında ücretli veya ücretsiz uygulamalar bulunmaktadır. Örn: Kaspersky Mobile Security, AVG Antivirus, Avast Antivirus, Eset Mobile Security vb. QR Kod bankacılık uygulamaları haricinde; kullanıcı adı, şifre, banka hesap bilgileri, kredi kartı bilgileri istememektedir. Eğer ki bu bilgileri isteyen bir siteye yönlendiriyorsa giriş yapılmaması ve herhangi bir bilgi verilmemesi gerekmektedir. Bu durumda QR Kodun yönlendirdiği URL'den şüphelenmek mümkündür (CSO From IDG Communications., 2011).

3.4. Görsel QR Kodlar

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 gömülebilmektedir (Lin ve diğerleri, 2015: 1515). Bu yöntem, değiştirilmiş QR Kodlarını tespit etmede kullanıcıyı önemli ölçüde desteklemektedir. Tema ne kadar karmaşık olursa, bir saldırganın QR Kodlarını göze batmayan bir şekilde değiştirmesi zorlaşmaktadır (Krombholz ve diğerleri, 2014: 7). Şekil 15'te Modüllerin rengi ve şekillerin değiştirilebildiği görsel yer almaktadır. Şekil 16'ta QR Koda içine gömülen resim, marka amblemi gibi görseller yer almaktadır.

Şekil 15. Modüllerin Rengini ve Şeklini Değiştirme

Şekil 16. Resim Gömme (Embedding a Picture) (Lin ve diğerleri, 2015: 1515).

Renkler, harfler, resimler veya logolar gibi üst düzey görsel özellikleri içeren kodlara Görsel QR Kodlar denmektedir. Görsellik olarak çekici olan QR Kodları üretmekte son yıllarda oldukça artış olmuştur. Ancak dikkat edilmesi gereken önemli nokta ise, okunabilirliğinden ödün vermeden görsel olarak ilginç bir QR Kodu oluşturmaktır. Chu ve diğerleri tarafından yüksek kalite görsel QR Kodlar üretebilmek için geliştirilen yarı tonlu QR Kod (Halftone QR Code) yaklaşımı önerilmiştir (Chu ve diğerleri, 2013: 1-8). Şekil 17' de oluşturdukları algoritma sayesinde yapılan üç adet yarı tonlu QR Kod verilmiştir.

Şekil 17. Oluşturulan üç yarı tonlu QR Kod Örnekleri (Chu ve diğerleri, 2013: 1-8).

3.5. Kimlik Doğrulama

Bankacılık uygulamalarında kullanılan, kimlik Doğrulama (One Time Password) yalnızca bir kez geçerli olarak oluşturulan paroladır. Kullanıcıya, algoritma ve şifreleme anahtarı kullanarak tek seferlik kullanabileceği parola verilmektedir. Kimlik Doğrulama sunucusu tarafından ise, aynı algoritma ve anahtar paylaşılarak şifrenin geçerliliğini kontrol edebilmektedir (Lee ve diğerleri, 2010: 644-645).

3.6. QR Kod Okuyucu Yazılımlar

Belirtilen saldırılar neticesinde, QR Kodun güvenilirliğini test eden yazılımlar geliştirilmiştir. Norton Snap QR Kod Okuyucu, Symantec Norton tarafından geliştirilen Android güvenlik uygulamasıdır. Kullanıcıları QR Kodu çevrimiçi tehditlerden korumayı amaçlayan bir QR Kod tarayıcı uygulamasıdır. Uygulama, QR Kodlarında kodlanmış URL'lerin güvenliğini kontrol etmektedir. Ardından kullanıcılara bu web sitesinin güvenli olup olmadığına dair tavsiyelerde bulunmaktadır. Web sitesi güvenli değilse, uygulama bu siteye erişimi engelleyecektir. QR ve Barkod okuyucu, barkodları güvenli bir şekilde okumayı amaçlayan diğer bir uygulamadır. Okuyucunun, iletişim bilgileri gibi kişisel bilgilere ulaşma izni yoktur (Bani-Hani ve diğerleri, 2014: 2).

KasperskyLab'ın Android için geliştirdiği QR Kod okuyucu ise, kötü amaçlı yazılımlara ve kimlik avı tuzaklarına maruz bırakmayacak tehlikeli bağlantılar içeren sahte QR Kodlarından koruyan akıllı bir QR Kod okuyucudur (Android Market-a, 2019). Trend Micro QR Tarayıcısı dolandırıcılık veya kötü amaçlı yazılım ve tehlikeli içeriklerden uzak güvenli bir web sitesine yönlendirilmenizi sağlayarak tüm kodlar üzerinde yüksek kaliteli URL güvenlik kontrolleri sunmaktadır (Android Market-b, 2019). SafeQR uygulaması, kimlik avı ve kötü amaçlı yazılım saldırıları için kullanılan kötü amaçlı URL'leri tespit etmenin etkinliğini artırmaktadır. Ayrıca bir QR Kodu tarandığında kullanıcının daha iyi karar verebilmesi için, güvenlik algısını artırmaktadır (Shin ve Yao, 2013: 50).

Bu bölümde QR Kod saldırılarına karşı alınabilecek önlemler verilmiştir. Bu çalışma ile ülkemizde eğitimli ve genç nüfusun bu saldırılara karşı farkındalık seviyesi ölçülmek istenmiştir. Çalışmanın temel araştırma sorusu toplumsal yaşamda bireylerin QR Kodların olası güvenlik zafiyetleri ve yaratacağı sorunlar hakkındaki farkındalık seviyelerinin tespit edilmesi üzerinedir.

IV. BÖLÜM: ARAŞTIRMA YÖNTEMİ

QR Kodların, kötü niyetli kişiler tarafından kimlik avı saldırılarında kullanılabileceğini göz önünde bulundurarak, kullanıcıların bu tür saldırılara karşı davranışları araştırılmak istenmiştir. Eğitimli kullanıcıların QR Kodları ile ilgili güvenlik konusunda ne derece bilgi sahibi oldukları belirlenmek istenilmiştir. Gördükleri herhangi bir QR Kodu tarayan kullanıcılar, bunun her zaman ki gibi risksiz bir işlem olmadığını fark edip etmediklerinin belirlenmesi hedeflenmiştir.

Bu çalışma ile insanların halka açık yerlerde bulunan QR Kodları taramadaki motivasyonlarının ne olduğunu anlamak ve QR Kodlar ile kimlik avı saldırısının ne kadar etkili olabileceği konusunda farkındalık yaratmak istenmiştir. Bu nedenle oluşturulan QR Kodlara URL vererek, bir web sitesine yönlendirilmiştir. Bu web sitesinde, QR Kodla ilgili hazırlanan güvenlik farkındalık anketini katılımcılardan doldurması istenilmiştir. Taratılan QR Kod sayesinde çevrimiçi anketimiz bir web tarayıcısında açılmaktadır.

Algılanan QR Kod güvenlik riskini ve bunun nasıl azaltılacağı üzerine çalışmada (Yin ve diğerleri, 2013) kullanıcıların QR Kod güvenlik riskleri konusundaki farkındalığını araştırmak ve kullanıcıların kötü niyetli QR Kodlarının uyarılarına nasıl yanıt vereceğini belirlemek için çevrimiçi bir anket uygulanmıştır. Anket sonuçları, bilgisayar ve teknolojide daha fazla deneyime sahip olan kullanıcıların, uyarı mesajlarını görmezden gelmelerinin daha muhtemel olduğunu ve kullanıcıların çoğunluğunun, QR Kod riskleri konusunda düşük düzeyde farkındalığa sahip olduğunu göstermiştir.

Yapılan benzer bir çalışma; (Kapsalis, 2013: 35-59) Viyana, Helsinki, Atina ve Paris şehirlerinde yapılmıştır. Aynı şekilde bir çevrimiçi anket ile farklı şehirlerde ve ülkelerde yapılmıştır. QR Kodlar Japonya'da, Avrupa'dan çok daha popülerdir. Çalışma, Tokyo'da da yapılmak istenmiş fakat, Ulusal Enformatik Enstitüsü Etik Bölümünden istenilen gereklilikler yerine getirilemediği için anket yapılamamıştır. QR Kod Saldırı senaryosu gerçeğe çok yakın şekilde tasarlanması ve kullanıcıların QR Kod etiketlerinin onları nereye yönlendirdiğini tam olarak bilmemeleri gerçeği Tokyo'daki çalışmayı imkânsız hale getirmiştir. Farklı konumlara yerleştirilen QR Kod etiketleri ile kullanıcılardan QR Kodun taratılması ve çevrimiçi anketin doldurulması istenmiştir. Bir web sitesi kullanılarak, web trafiği de gözlenmiştir (Kapsalis, 2013: 35-59).

Bu çalışma da ise; sade, talimatlı ve resimli olarak üç farklı QR Kod Afişi hazırlanmıştır. Bu afişler Ankara ilinde, Başkent Üniversitesi Bağlıca Kampüsü ve Hacettepe Teknokent'e asılmıştır. Teknoloji ile iç içe, belli bir bilgi birikimi sahibi olan genç nesil hedef kitlesi olarak seçilmiştir.

4.1. Çevrimiçi Anket

Bu çalışmada Ioannis Kapsalis'in (2013) QR Kod ölçeği birebir Türkçe'ye çevrilmek suretiyle kullanılmıştır. 5 adet QR kod ile ilgili soru ve 2 adet demografik sorular ile toplamda 7 adet soru ankette yer almaktadır. Anket, katılımcılarla etkileşim açısından önemlidir. Katılımcıları sorular ile boğmamak, formu doldururken sıkılmamaları için, 3 dakika da doldurabilecekleri basit ve kısa bir ankettir. Google Forms, ücretsiz çevrimiçi anket olarak kullanılabilecek formlar oluşturabildiğimiz bir hizmet sunmaktadır. Ayrıca, anketin otomatik olarak bir elektronik tablo ile ilişkilendirilmiş olması, cevapların izlenmesini kolaylaştırdığı için tercih edilmiştir. Bir katılımcı çevrimiçi ankete ulaştığında, anketin amacının ne olduğu hakkında bilgi ve QR Kodu tarattıkları için teşekkür mesajı almaktadır.

Araştırma için oluşturulan QR Kodlar, akıllı telefonlar aracılığıyla taratıldığı zaman bir web sitesine yönlendirmektedir. Açılan bu web sayfasında çevrimiçi anket yer almaktadır. "Google Forms" yardımıyla oluşturulan bu anket, Tablo 2 de yer almaktadır. Araştırmada anket sorularının tümüne cevap istenildiği için, Google Forms'da sorulara "gerekli" seçeneği seçilmiştir. Böylelikle toplamda 7 soru bulunan anket, tüm sorular cevaplanmadan tamamlanmayacaktır.

Tablo 2. Anket Soruları ve Şıkları

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.

Katılımcılara ankette sorulan ilk soru, “Bu QR Kodu neden taradınız?” sorusudur. Bu soru katılımcıların motivasyonunu ortaya çıkarmak için sorulmuştur. İlk soruda cevaplar arasında “Merak Ediyordum” seçeneği yer almaktadır. Merak çoğu durumda, insanların bir QR Kodu taramasının nedenidir. QR Kod afişlerini oluştururken de bu konu göz önüne alınmıştır. Bazı QR Kod afişlerinin yanına ilgi çekici resimler konulmuştur. Bu yüzden cevaplar arasına “resim ilgimi çekti” seçeneği vardır. QR Kodun altında “Bu QR Kodu taramak için…:” bilgi bulunan yani nasıl taratılması gerektiği hakkında bilgi veren ve yönlendiren afiş içinse “ilgili bilgi beni çekti” cevabı yer almaktadır. Geri kalan cevaplar ise; “sıkılmıştım”, “QR Kodun ne olduğunu bilmiyorum”, “cevap vermek istemiyorum” ve “Diğer:…” şeklindedir. Katılımcıların cevap vermeme haklarının da bulunduğu gibi aynı zamanda kendileri de bir şeyler eklemek isteyenler için “diğer” kısmı yazı yazılacak şekilde ayarlanmıştır. Burada katılımcılardan farklı şekillerde geri dönüşler sağlanması durumunda soruya katkıda bulunacaklardır.

Çevrimiçi anketin ikinci sorusu, katılımcıların bir QR Kodu taramadan önce herhangi bir şüpheleri olup olmadığını veya herhangi bir kötü amaçlı içerik bekleyip beklemediklerini içeren sorudur. QR Kodun nereye yönlendirdiğini bilmediklerinden, bir QR Koduyla kötü amaçlı içeriğe erişebileceklerini akılda tutmaları sağlanmak istenilmiştir.

Diğer bir soruda, katılımcıların ***Phishing “Kimlik Avı”*** saldırısının kurbanı olup olmadığı sorulmuştur. Böylece katılımcıların, bilgi teknolojileri (BT) güvenliği konusunda geçmişe dair bilgiler vereceği düşünülmüştür. Aynı zamanda, QR Kodlara aşina olan katılımcıların bilgilerinin seviyeleri hakkında da bilgi edinilebileceği düşünülmüştür.

Ayrıca katılımcılara QR Kodları ne sıklıkla taradıkları sorulmuştur. Bu sorudan elde edilen veriler, katılımcıların QR Kodlarına aşinalıklarıyla güvenlik farkındalığı düzeyleri arasında bir ilişki olup olmadığını doğrulamasına yardımcı olacaktır. Tarama sıklığı hakkında toplanan bilgiler ayrıca QR Kodlarının kabulüne ve kullanımına genel bir bakış sağlamaktadır.

Katılımcıların yaşı ve cinsiyeti hakkında bilgi toplamak için demografik sorular da ankette yer almaktadır. Bu bilgiler, yaş ve cinsiyete bağlı olarak güvenlik bilincinin ve seviyesinin nasıl etkilendiğine dair çıkarımlarda bulunmaya yardımcı olacaktır. Beklenti, genç katılımcıların bu ankette aktif olmalarıdır. Ancak yaşam boyu öğrenme eğilimleri ile alınan eğitim ve yaşanılan tecrübeleri de keşfetmek gereklidir.

Ankette, bazı sorularda katılımcılar “Cevap vermek istemiyorum” seçeneğini seçerek, soruyu atlayabilmesi sağlanmıştır. Bir sorunun onlar için çok hassas veya uygunsuz olduğuna inanmaları ve herhangi bir bilgi vermemeyi tercih etmeleri durumu için katılımcılara bu seçenek verilmiştir.

QR Kodu taratıp web sayfasına yönlendirildikten sonra anket formunu doldurmama gibi problemler için web trafiği izlenmiştir. Bu sebeple “Google Analytics” kullanılmıştır. Google tarafından sunulan ücretsiz bu hizmet, katılımcıların; sitenizin ne kadar sıklıkla ziyaret edildiği, lokasyonu, sayfada vakit geçirme ve ortalama geçirdiği süre bilgisi, hemen çıkma oranı (sayfayı ziyaret eden katılımcıların hızlı bir şekilde çıkmaları), mobil cihazdan mı yoksa masaüstü bilgisayardan mı giriş yapıldığı hakkında bilgiler vermektedir. Ayrıca bu bilgilere günlük, aylık ve saatlik olarak ulaşılabilmektedir.

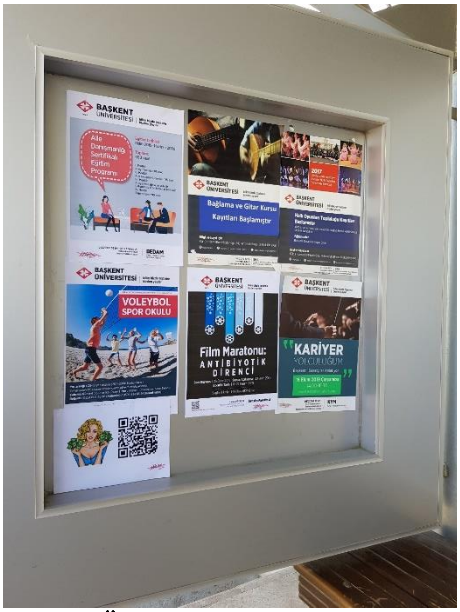
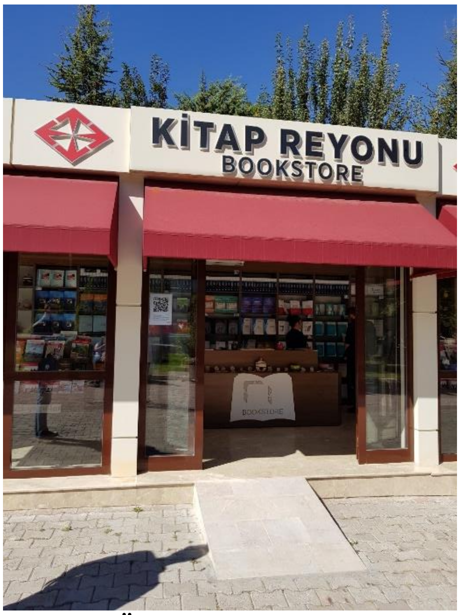
Google Analitik, web sayfasının trafiğini, doldurulan anket soruları ve doldurulmadan çıkan kişilerin ayırt edilmesi gibi bilgileri sağlamaktadır. Çalışmada kullanılan web sitesi, Başkent Üniversitesi’nin öğrencilerine belli bir boyut dahilinde ücretsiz olarak sağladığı alan adıdır. 3 adet farklı QR Kod için (sade, talimatlı, resimli), 3 farklı URL bağlantı oluşturulmuş böylece her bir QR Kod için istatistikler ayrı ayrı hesaplanmıştır.

4.2. Lokasyon ve Hedef Gruplar

Lokasyon olarak Türkiye, Ankara ili, Başkent Üniversitesi Bağlıca Kampüsü ve Hacettepe Teknokenti seçilmiştir. Başkent Üniversitesi Bağlıca Kampüsünde, 1085 öğretim elemanı ile 14804 öğrenci bulunmaktadır (Başkent Üniversitesi, 2019). Afişler üniversitede 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 (Hacettepe Teknokent, 2019). Teknoloji okur-yazarı olan ve akıllı mobil cihaz kullanan genç nesil hedef kitlesi olarak seçilmiştir.

Başkent Üniversitesi Bağlıca Kampüsü ve Hacettepe Teknokent duyuru panoları, kafeterya ve servis duraklarına asılan afiş fotoğrafları Tablo 3'de yer almaktadır.

Tablo 3. Asılan QR Kod Afişleri

<table>
<tr>
<td>Hacettepe Teknokent Panosu</td>
<td>Başkent Üniversitesi Servis Durakları</td>
</tr>
<tr>
<td>Başkent Üniversitesi Kitap Reyonu</td>
<td>Başkent Üniversitesi, Sosyal Bilimler Enstitüsü Duyuru Panosu</td>
</tr>
</table>

4.3. Çalışma Kısıtları

Çalışma, hedef kitlesi kapsamındaki Ankara ilinde bulunan diğer üniversite ve teknokentlerde de uygulanmak istenmiş fakat bazı prosedürler/izinler gerekliliği ile karşılaşılmıştır. İlgini başvuruların yapılmasına rağmen sonuç alınamadığı için çalışmada sadece Başkent Üniversitesi ve Hacettepe Teknokent ile sınırlı kalınmıştır.

4.4. QR Kod Afişleri

Çalışma dahilinde, aşağıda detayları verilen 3 farklı QR Kod tasarlanmıştır.

4.4.1. Sade QR Kod Afişi

Siyah beyaz renkte, en sade şekliyle olan QR Kod afişlerinin kişiler tarafından ilgi çekmesi ve okutulma sayısına bakılması için yanında hiçbir bilgi ve başka resim içermeyen haliyle asılmıştır. Sade QR Kod: https://mail.baskent.edu.tr/~21710225/normal/ linkine gitmektedir. Şekil 18'de Sade QR Kod afişi yer almaktadır.

Şekil 18. Sade QR Kod Afişi

4.4.2. Talimatlı QR Kod Afişi

Bu Afişte QR Kodun altında, QR Kodun nasıl taratıldığını anlatan bir açıklama yer almaktadır. Bu açıklama ile kodu taramak isteyen kişiler, buradaki yönlendirmeye uyarak kodu tarayabilirler. Daha önce QR Kodu taramamış, bu konu hakkında bilgi sahibi olmayan ve deneyimsiz katılımcıların herhangi bir problem yaşamadan QR Kodu taramalarının sağlanması amaçlanmıştır. Talimatlı olan QR Kod: https://mail.baskent.edu.tr/~21710225/tanimli/ linkine gitmektedir. Şekil 19'da Talimatlı QR Kod afişi yer almaktadır.

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.

Şekil 19. Talimatlı QR Kod Afişi

4.4.3. Resimli QR Kod Afişi

QR Kodun yanında ilgi çeken ve merak uyandıran resimler kullanılmıştır. Seçilen resimler, insanların ilgisini çekecek para, parti, ödül gibi çağrışımlar içermektedir. Seçilen resimlerin diğer QR kod afişlerine göre daha fazla merak uyandırıp QR Kodun taratma sayısında anlamlı bir artış gerçekleştirmesi beklenmiştir. Merak duygusunun, kişilerin başına açacağı sorunlara rağmen taratılmasının ve bunun güvenlik zafiyeti oluşturduğu gösterilmek istenmiştir. Resimli olan QR Kodlar: https://mail.baskent.edu.tr/~21710225/resimli/ linkine gitmektedir. Şekil 20 ve Şekil 21'de Resimli QR Kod afişleri yer almaktadır.

Şekil 20. Resimli QR Kod Afişi 1

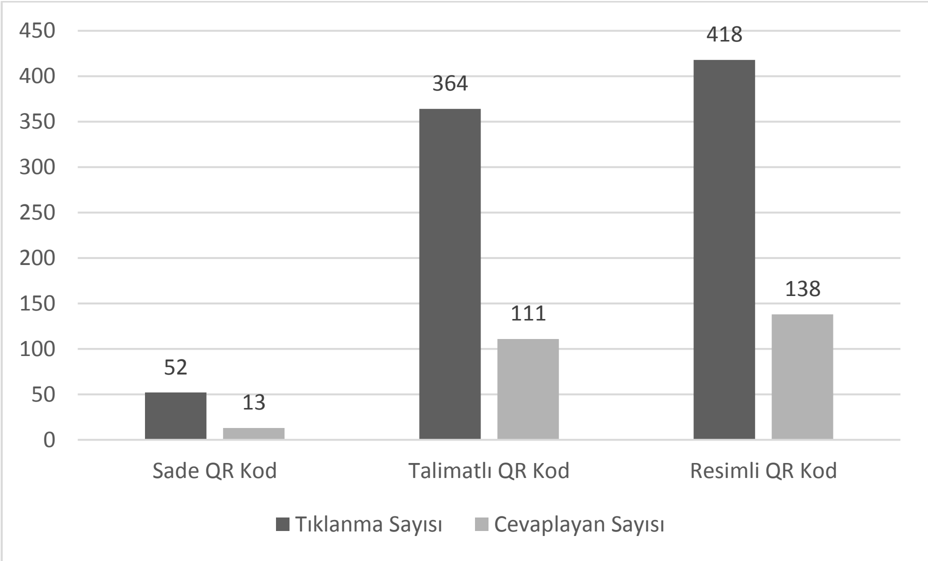
Şekil 21. Resimli QR Kod Afişi 2

V. BÖLÜM: ANALİZ VE BULGULAR

QR Kodların değiştirilebilmesi ve 1.4.'te belirtilen QR Koda saklanabilecek veri miktarına bakıldığında, kötü niyetli kişiler tarafından kimlik avı saldırısında bir saldırı vektörü olarak kullanılabilmektedir. Bu nedenle, çevrimiçi anket kullanılarak katılımcılardan veriler toplanmıştır. Toplanılan verilere göre ulaşılan sonuçlar bu kısımda belirtilmiştir.

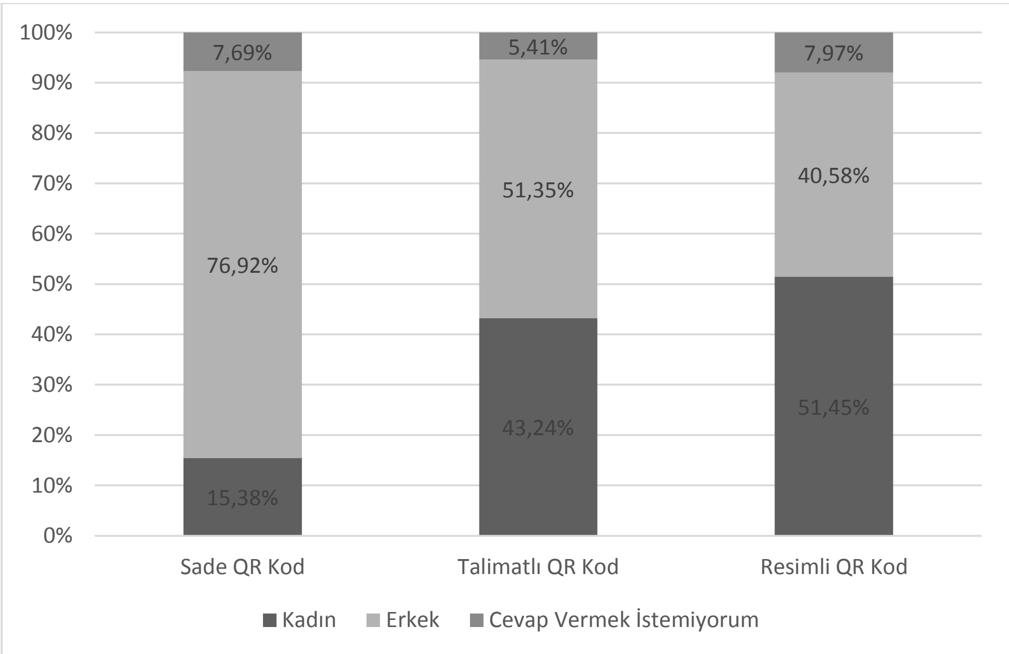
Teknokent ve Üniversitede yapılan anket çalışmasında QR Kodları içeren afişler 40 gün (3 Ekim 2019 - 11 Kasım 2019) boyunca asılı kalmıştır. Daha öncede belirtildiği gibi QR Kodların cevaplarını toplamak için "Google Forms" kullanılmıştır. Ek olarak, web sayfası trafiği izlemek içinde "Google Analytics" kullanılmıştır. Hacettepe Teknokent'de Dört Blok içinde bulunan genel duyuru panolarına her bir panoya bir adet asılacak şekilde toplamda 3 adet QR Kod afişi asılmıştır. Başkent Üniversitesinde; 14 adet genel pano (servis durakları ve genel geçilen yerler), 26 adet fakülte ve enstitü panoları, 17 adet ise kafeterya, kırtasiye, market ve yemekhane olmak üzere toplamda 57 adet QR Kod afişi asılmıştır. Teknokent ve Üniversite ile birlikte asılan toplam QR Kod afiş miktarı 60 adettir. Asılan QR Kod afişleri Sade, Talimatlı ve Resimli sayısı eşit olacak şekilde dağıtım yapılmıştır.

QR Kod afişinin yönlendirdiği web adresinin tıklanma sayısı ve anketi cevaplayan sayısını gösteren Şekil 22'den anlaşılacağı üzere; sade QR Kod afişi yönlendirdiği web adresi 52 kişi (%6,24) tarafından tıklanmış ama cevaplayan kişi sayısı 13'tür (%1,56). Talimatlı QR Kodun yönlendirdiği web adresine tıklayan sayısı 364 kişi (%43,65), cevaplayan sayısı 111 kişidir (%13,31). Resimli QR Kod afişinin yönlendirdiği web adresi tıklanma sayısı 418 kişi (%50,12), anketi cevaplayan sayısı ise 138 kişidir (%16,55). Toplamda web adresini 834 kişi ziyaret etmiş, 262 kişi ise anketi cevaplamıştır (%31,41). Buradan 572 kişinin (%68,59) anketi gördüğü ama doldurmadığı ortaya çıkmaktadır.



Şekil 22. Tıklanma Sayısı ve Anketi Cevaplayan Sayısı

Katılımcıların Cinsiyet grafiği Şekil 23'de verilmiştir. Sade QR Kod anketine katılanların %15,38'i kadın, %76,92'si erkek ve %7,69'u cinsiyet belirtmek istememiştir. Talimatlı QR Kod anketine katılanların %43,24'ü kadın, %51,35'i erkek ve %5,41'ü Cinsiyet belirtmek istememiştir. Resimli QR Kod anketine katılanların %51,45'i kadın, %40,58'i erkek, %7,97'si cinsiyet belirtmek istememiştir.

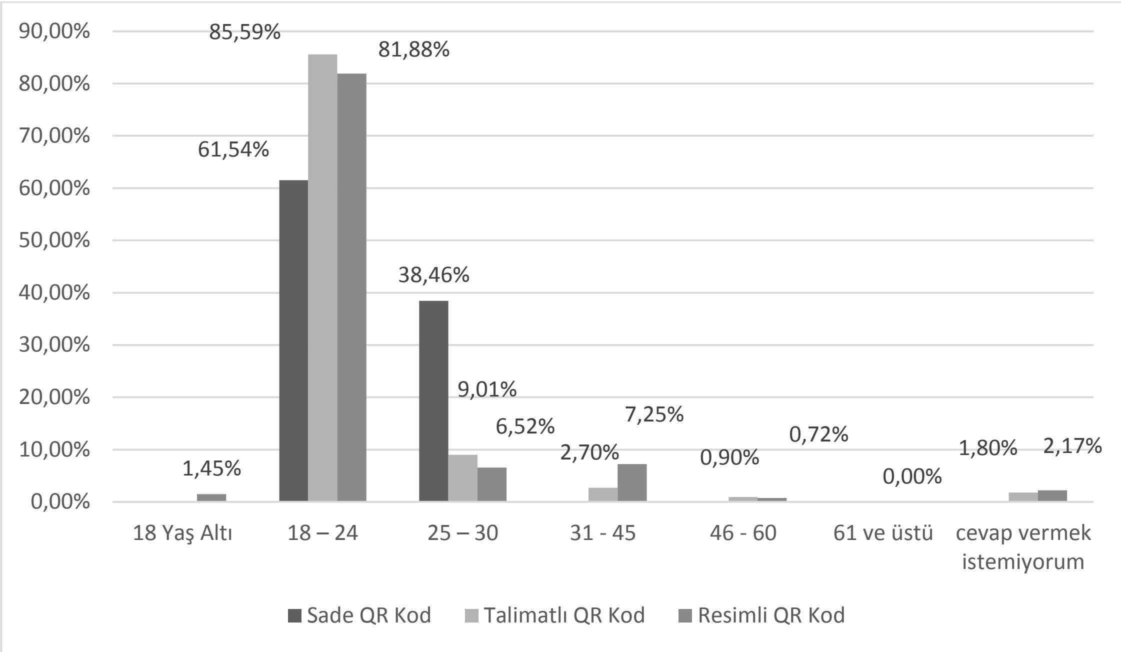


Şekil 23. Cinsiyet Grafiği

Toplamda anketimize katılan kadın sayısı 121'dir. Erkek sayısı 123'tür. Cinsiyet belirtmek istemeyen kişi sayısı 18'dir. Buna göre toplamda kadınlar %46,1'lık kısmı, erkekler %46,9'luk kısmı ve cevap vermek istemeyenler ise %7'lik kısmı oluşturmaktadır. Kadın ve erkek katılımcı sayısı birbirine çok yakındır.

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. Burada kadınların Resimli QR Kodu tercih etmelerini onlar için dikkat çekici unsurun QR Koda yerleştirilen "parti" ve "para" görselleri olduğu düşünülmektedir.

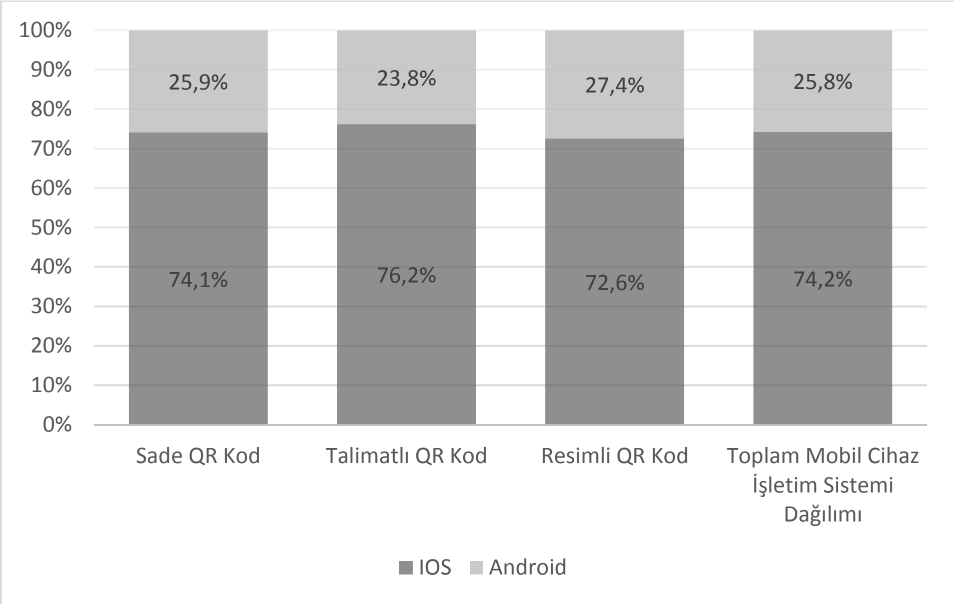
Ankete katılan kişilerin yaş grafiği Şekil 24'de verilmiştir. Sade QR Kod afişini cevaplayanların, %61,54'lük kısmı 18-24 yaş aralığı yani 8 kişi, %38,46'lık kısmı ise 25-30 yaş aralığında yani 5 kişidir. Talimatlı QR Kod afişini cevaplayanların %85,59'luk çoğunluğu 18-24 yaş aralığındadır. %9,01'lik kısmı 25-30 yaş aralığındadır. %2,70'lik kısmı 31-45 yaş aralığındadır. %0,90'lık kısım ise 46-60 yaş aralığındadır. %1,80'lik kısım yaş belirtmek istememiştir. Resimli QR Kod afişinin yaş ölçeğine bakıldığında, %81,88'lik çoğunluk 18-24 yaş aralığındadır. 25-30 yaş aralığında bulunanlar %6,52 ve 31-45 yaş aralığında bulunanlar %7,25'lik orana sahiplerdir. Yaş soruna cevap vermek istemeyen kişi sayısı 3 kişi olup %2,17'lik orana sahiptir. %0,72'lik kısım da 46-60 yaş aralığındadır. Aynı zamanda %1,45'lik oranla 18 yaş altı (2 kişi) katılım gerçekleşmiştir.



Şekil 24. Yaş Grafiği

Resimli, talimatlı veya sade QR Kod dahil olarak, toplamda 18 yaş altı 2 katılımcı, 18-24 yaş aralığı 216 katılımcı, 25-30 yaş aralığı 24 katılımcı, 31-45 yaş aralığı 13 katılımcı, 46-60 yaş aralığı 2 katılımcı katılmıştır. 61 ve üstü yaş aralığında anketimize katılan olmamıştır. Yaş belirtmek istemeyen toplam kişi sayısı ise 5 kişidir. 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.

Katılımcılar, toplamda %74,2 oranında IOS işletim sisteminden, geriye kalan %25,8 ise Android işletim sisteminden giriş yapıp ankete katılmıştır. Windows Mobile veya Blackberry vb. işletim sistemi kullanan mobil cihazlardan katılım olmamıştır. En yüksek oran Şekil 25'de görüldüğü üzere IOS işletim sistemi ile Apple'a aittir.



Şekil 25. Mobil Cihaz İşletim Sistemi Dağılımı

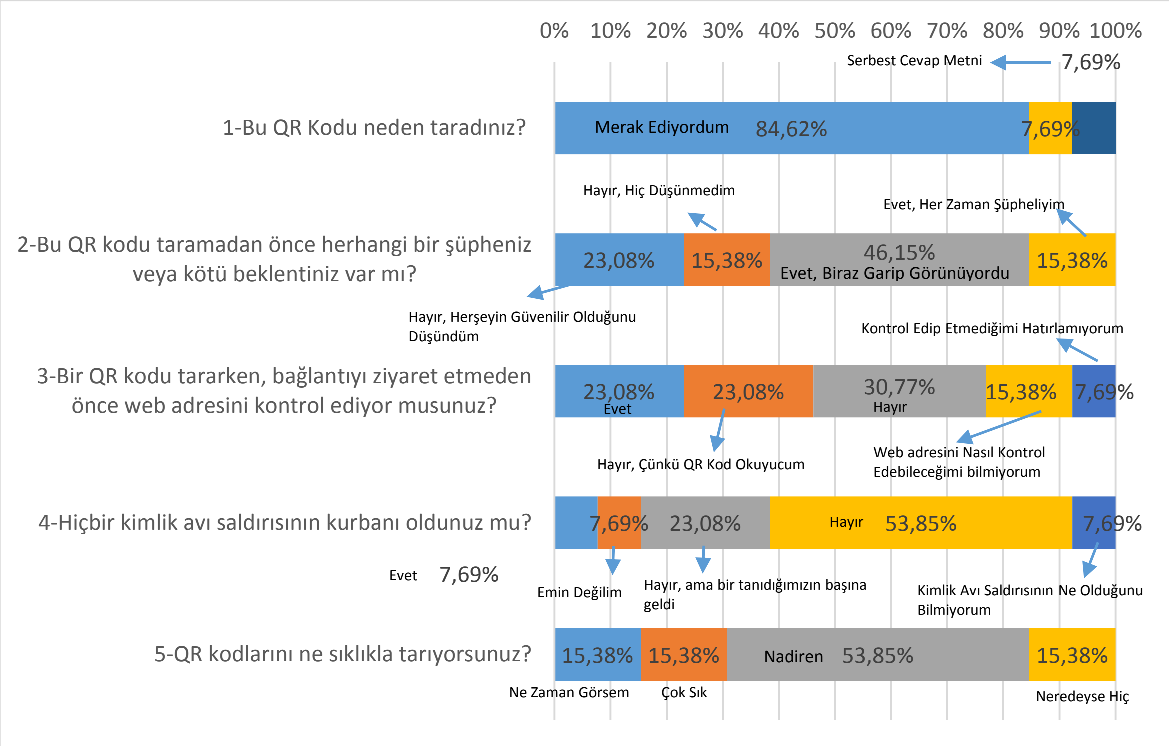
5.1. Sade QR Koda İlişkin Analiz

Sade QR Kod sonuçları Şekil 26'da görüldüğü üzere, "Bu QR Kodu neden taradınız?" sorusuna katılımcılar tarafından, en fazla "Merak ediyordum" cevabı verilmiştir. Ankete cevap veren katılımcıların çoğu %84,62'lik oranla QR Kodu en çok meraktan taramışlardır. %7,69'luk kısmı "sıkılmıştım" yanıtını vermiştir. Geriye kalan %7,69 ise, serbest cevap metni olan "Diğer:…" seçeneğini seçerek, üstteki afişin resmini çekerken bildirim gelip ankete katıldığını belirtmiştir. Herhangi bir bilgi veya tanımlama içermediği için "İlgili bilgi beni çekti" seçeneği hiç seçilmemiştir. "Resim ilgimi çekti", "QR Kodun ne olduğunu bilmiyorum" ve "Cevap vermek istemiyorum" şıkları da yanıtlanmamıştır. Herhangi bir bilgi veya resim kullanmadan, katılımcılara ipucu verilmeden olduğu gibi QR Kod asılmıştır. Rastgele bir QR Kodu taramak, tahmin edilemeyen bir içeriğe erişmeye ve tamamen bilinmeyen bir web sitesine ziyaret etmek anlamına gelmektedir. İnsanların merakını takip etmesi zararlı olabilmektedir.

Şüpheyle ilgili olan ikinci soruda, en çok cevap alan şık %46,15'lik oranla "Evet, biraz garip görünüyordu" cevabıdır. Katılımcılar tarafından tuhaf bir görüntü olduğu kabul edilmiş ancak yine merak duygusu ön plana çıkmaktadır. %15,38'i ise "Evet, her zaman şüpheliyim" cevabını seçmiştir. Cevap verenlerin %15,38'i "Hayır, hiç düşünmedim" cevabını seçerek kötü bir beklenti içerisinde olmadığını belirtmiştir. Katılımcıların %23,08'i her şeyin güvenli olduğunu düşünmüştür.

Üçüncü soruda, katılımcılara web adreslerini kontrol edip etmedikleri sorulmuştur. Hayır cevabı vererek %30,77'lik kısımla web sitesini kontrol etmeyenler çoğunluktadır. Web sitesini kontrol etmedikleri için insanların kolayca saldırıya uğrayabilecekleri anlaşılmıştır. QR Kod okuyucusu bağlantıyı otomatik ziyaret edenlerin oranı %23,08'dir. Bazı okuyucularda web sayfa adresini gösterip bildirime tıkladıktan sonra ziyaret edilmektedir. Web Sayfasının otomatik olarak ziyaret edilmesi demek kötü niyetli kişilerin işini kolaylaştıracaktır. Web adresini nasıl kontrol edebileceğini bilmeyen kişi oranı %15,38'dir. Kontrol edip etmediğini hatırlamıyorum cevabını verenlerin oranı ise %7,69'dur. Web sitesi kontrol eden yani "Evet" yanıtını verenlerin oranı %23,08'dir.

Dördüncü soruda, katılımcılara daha önce kimlik saldırısına uğrayıp uğramadıkları sorulmuştur. %53,85'lik kısım yani büyük bir çoğunluk, "Hayır" cevabını vererek saldırıya uğramadıklarını belirtmiştir. "Hayır, ama tanıdığımızın başına geldi" cevabını verenlerin oranı ise %23,08'dir. Cevaplar arasında, katılımcıların mağdur olmaktan utanabilecekleri ve bir yandan bu konuda bilgisiz olduklarını söylemeye çekinebilecekleri için böyle bir şık vardır. Kimlik avı saldırısı kurbanı olanların yüzdesi ise %7,69'dur. Saldırıya uğrayıp uğramadıklarından emin olamayan oranı %7,69 ve kimlik avı saldırısının ne olduğunu bilmeyenlerin oranı da %7,69'dur. Yani %15,38'lik kısım kimlik avı saldırısı hakkında tam olarak bilgi sahibi olmadığı gözükmektedir. Cevap vermek istemiyorum cevabı hiç seçilmemiştir.



Şekil 26. Sade QR Kod Cevaplama Oranları

Katılımcılara beşinci soruda; QR Kodlarına aşina oldukları keşfetmek amacıyla, QR Kodlarını tarama sıklıkları sorulmuştur. Ek olarak QR Kodun kendisini yeni bir teknoloji olarak insanlara kabul ettirmesini ve bunu ne derece başardığı belirlenmiştir. Büyük çoğunluk yani %53,85'lik kısım QR Kodları "Nadiren" taradığı cevabını vermiştir. Geriye kalan şıklar eşit şekilde cevaplanarak, "Ne Zaman görsem", "Çok Sık" ve "Neredeyse hiç" şıklarının hepsi %15,38'lik cevaplanma oranına sahiptir. "Çok sık" ve "Neredeyse hiç" gibi birbirine zıt iki şıkta aynı oranda cevap almıştır.

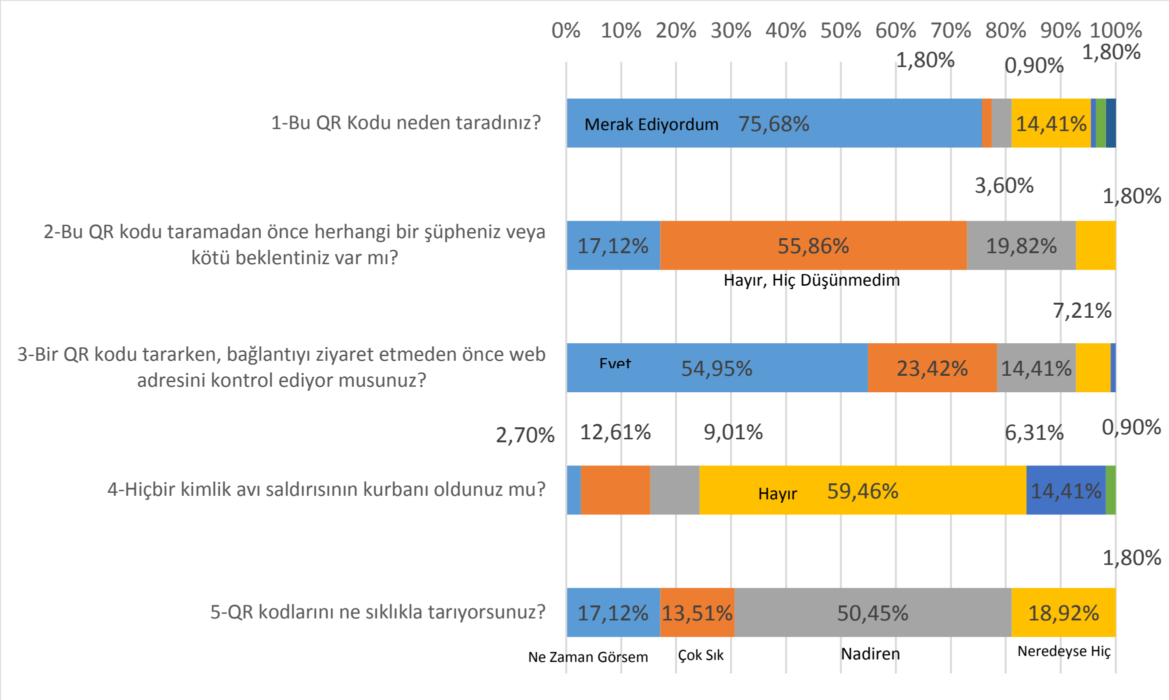
5.2. Talimatlı QR Koda İlişkin Analiz

Talimatlı QR Kod sonuçları Şekil 27'de görüldüğü üzere, "Bu QR Kodu neden taradınız?" sorusuna katılımcılar tarafından, en fazla "Merak ediyordum" cevabı verilmiştir. Ankete cevap veren katılımcıların çoğu %75,68'lik oranla QR Kodu en çok meraktan taramışlardır. %3,60'lık kısmı "Resim ilgimi çekti" yanıtını vermiştir. Siyah beyaz orijinal halde QR Kod ile birlikte, kodu taramak için altında tanımlama yer alan afiş, katılımcılar tarafından ilgi çekmiştir. "Sıkılmıştım" yanıtını verenler %14,41'lük kısmı oluşturmaktadır. "İlgili bilgi beni çekti" cevabı %1,80'lik oranla cevaplanmıştır. Soruya cevap vermek istemeyen katılımcılar da %1,80'lik oran oluşturmaktadır. QR Kodun ne olduğunu bilmeyen ise %0,90'dır. Diğer seçeneğini seçip, kendisi cevap vermeyi tercih eden katılımcılar (%1,80); QR Kodun Kocaman olduğundan dolayı merak ettiklerini ve virüs programının aktif olduğunu yazmışlardır. Altında tanımlama olmasına rağmen, QR Kodu resim olarak düşünüp bu yüzden "Resim ilgimi çekti" yanıtı daha fazla verilmiştir.

Şüpheyle ilgili olan ikinci soruda, en çok cevap alan şık %55,86'lık oranla "Hayır, hiç düşünmedim" yanıtıdır. %7,21 ise "Evet, her zaman şüpheliyim" cevabını seçmiştir. Cevap verenlerin %19,82'i "Evet, Biraz garip görünüyordu" cevabını vermiştir. Katılımcıların %17,12'si her şeyin güvenliği olduğunu düşünmüştür. QR Kodun altında bir yazı bulunması, hiç düşünmeden yazıya güvenip QR Kodu okutanların çoğunlukta olduğunu göstermektedir.

Üçüncü soruda, katılımcılara web adreslerini kontrol edip etmedikleri sorulmuştur. %54,95'lik oranla en çok cevap alan "Evet" seçeneği seçilmiştir. QR Kod okuyucusu bağlantıyı otomatik ziyaret edenlerin oranı %23,42'dir. Web sitesi kontrol etmeyen "Hayır" yanıtını verenler %14,41'dir. Web adresini nasıl kontrol edebileceğini bilmeyen kişi oranı %6,31'dir. Kontrol edip etmediğini hatırlamıyorum cevabını verenlerin oranı ise %0,90'dır.

Dördüncü soruda, katılımcılara daha önce kimlik saldırısına uğrayıp uğramadıkları sorulmuştur. %59,46'lık kısım yani büyük bir çoğunluk, "Hayır" cevabını vererek saldırıya uğramadıklarını belirtmiştir. "Hayır, ama tanıdığımızın başına geldi" cevabını verenlerin oranı ise %9,01'dir. Kimlik avı saldırısı kurbanı olanların yüzdesi ise %2,70'dir. Saldırıya uğrayıp uğramadıklarından emin olamayan oranı %12,61 ve kimlik avı saldırısının ne olduğunu bilmeyenlerin oranı da %14,41'dir. Cevap vermek istemiyorum yanıtını seçenlerin oranı %1,80'dir.



Şekil 27. Talimatlı QR Kod Cevaplanma Oranları

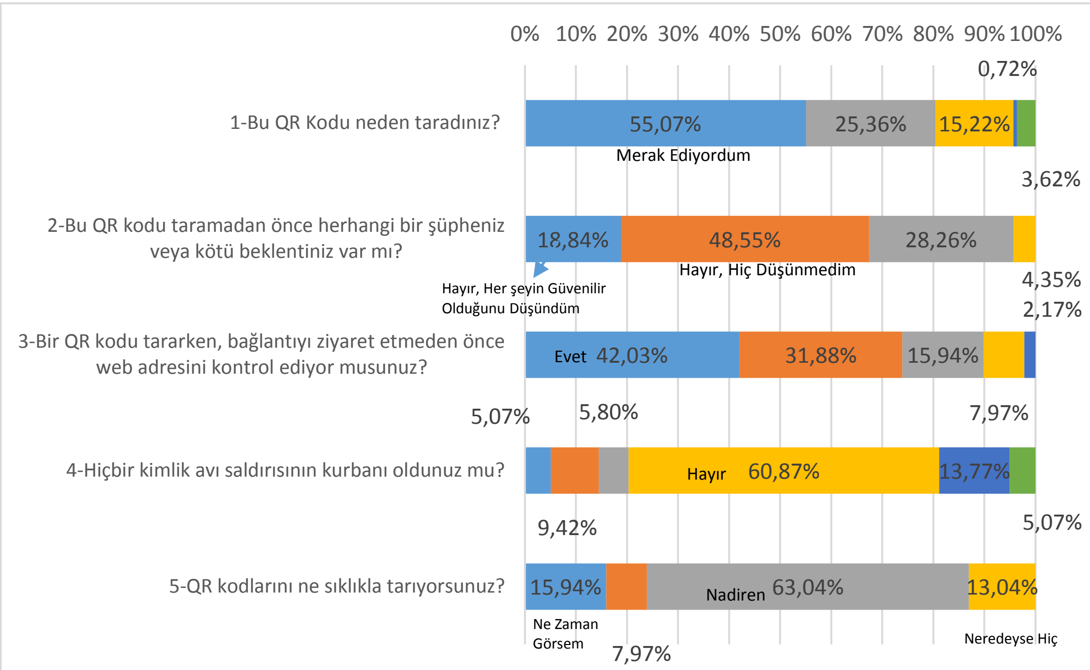
Katılımcılara beşinci soruda, cevap veren katılımcıların yarısı yani %50,45'i QR Kodları "Nadiren" taradığı cevabını vermiştir. "Ne Zaman görsem" yanıtını seçen %17,12, "Çok Sık" yanıtını seçen %13,51 ve "Neredeyse hiç" yanıtını seçen %18,92'lik oranlara sahiptir.

5.3. Resimli QR Koda İlişkin Analiz

Resimli QR Kod sonuçları Şekil 28'de görüldüğü üzere, "Bu QR Kodu neden taradınız?" sorusuna katılımcılar tarafından, diğer QR Kod afişlerindeki gibi en fazla "merak ediyordum" cevabı verilmiştir. Ankete cevap veren katılımcıların çoğu (%55,07) QR Kodu merak ettikleri için taramışlardır. %25,36'lık kısmı "Resim ilgimi çekti" yanıtını vermiştir. QR Kodun yanında kadın, para ve partiye hazır gibi resimlerin bulunması ilgi çekmesine neden olmuştur. En yüksek merak seçeneği seçilmesine rağmen, resim bulunan QR Kodlar diğer afişlere göre en çok tıklanan (416 ziyaretçi) ve yanıtlanan anket (138) afişi olmuştur. "Sıkılmıştım" yanıtını verenler %15,22'lik kısmı oluşturmaktadır. "İlgili bilgi beni çekti" cevabı hiç yanıt almamıştır. Soruya cevap vermek istemeyen katılımcılar da %3,62'lik oran oluşturmaktadır. QR Kodun ne olduğunu bilmeyen ise %0,72'dir. Kendi yanıtını paylaşması istenilen serbest cevap seçeneği hiç seçmemiştir.

Şüpheyle ilgili olan ikinci soruda, en çok cevap alan şık %48,55'lik oranla "Hayır, hiç düşünmedim" yanıtıdır. Kadın ve para resimleri, ödül kazanmak cinsellik gibi konuları çağrıştırıp bir ön bilgi verdiği düşüncesi ile şüphe uyandırmamıştır. %4,35'i "Evet, her zaman şüpheliyim" cevabını seçmiştir. Yani bir kısım ise şüpheci davranmıştır. Cevap verenlerin %28,26'sı "Evet, Biraz garip görünüyordu" yanıtını vermiştir. Katılımcıların %18,84'ü her şeyin güvenliği olduğunu düşünmüştür.

Üçüncü soruda, katılımcılara web adreslerini kontrol edip etmedikleri sorulmuştur. %42,03'lük oranla en çok işaretlenen "Evet" seçeneği olmuştur. QR Kod okuyucusu bağlantıyı otomatik ziyaret edenlerin oranı %31,88'dir. Web sitesi kontrol etmeyen "hayır" yanıtını verenler %15,94'dür. Web adresini nasıl kontrol edebileceğini bilmeyen kişi oranı %7,97'dir. Kontrol edip etmediğini hatırlamıyorum cevabını verenlerin oranı ise %2,17'dir.



Şekil 28. Resimli QR Kod Cevaplanma Oranları

Dördüncü soruda, katılımcılara daha önce kimlik saldırısına uğrayıp uğramadıkları sorulmuştur. %60,87'lik kısım yani büyük bir çoğunluk, "Hayır" cevabını vererek saldırıya uğramadıklarını belirtmiştir. "Hayır, ama tanıdığımızın başına geldi" cevabını verenlerin oranı ise %5,80'dir. Kimlik avı saldırısı kurbanı olanların yüzdesi ise %5,07'dir. Saldırıya uğrayıp uğramadıklarından emin olamayan oranı %9,42 ve kimlik avı saldırısının ne olduğunu bilmeyenlerin oranı da %13,77'dir. Cevap vermek istemiyorum yanıtını seçenlerin oranı %5,07'dir.

Katılımcılara beşinci soruda, cevap veren katılımcıların yarısından fazlası yani %63,04'lük kısmı QR Kodları "Nadiren" taradığı cevabını vermiştir. "Ne Zaman görsem" yanıtını seçen %15,94, "Çok Sık" yanıtını seçen %7,97 ve "Neredeyse hiç" yanıtını seçen %13,04'lük oranlara sahiptir.

5.4. QR Kod Afişlerin Toplamına İlişkin Analiz

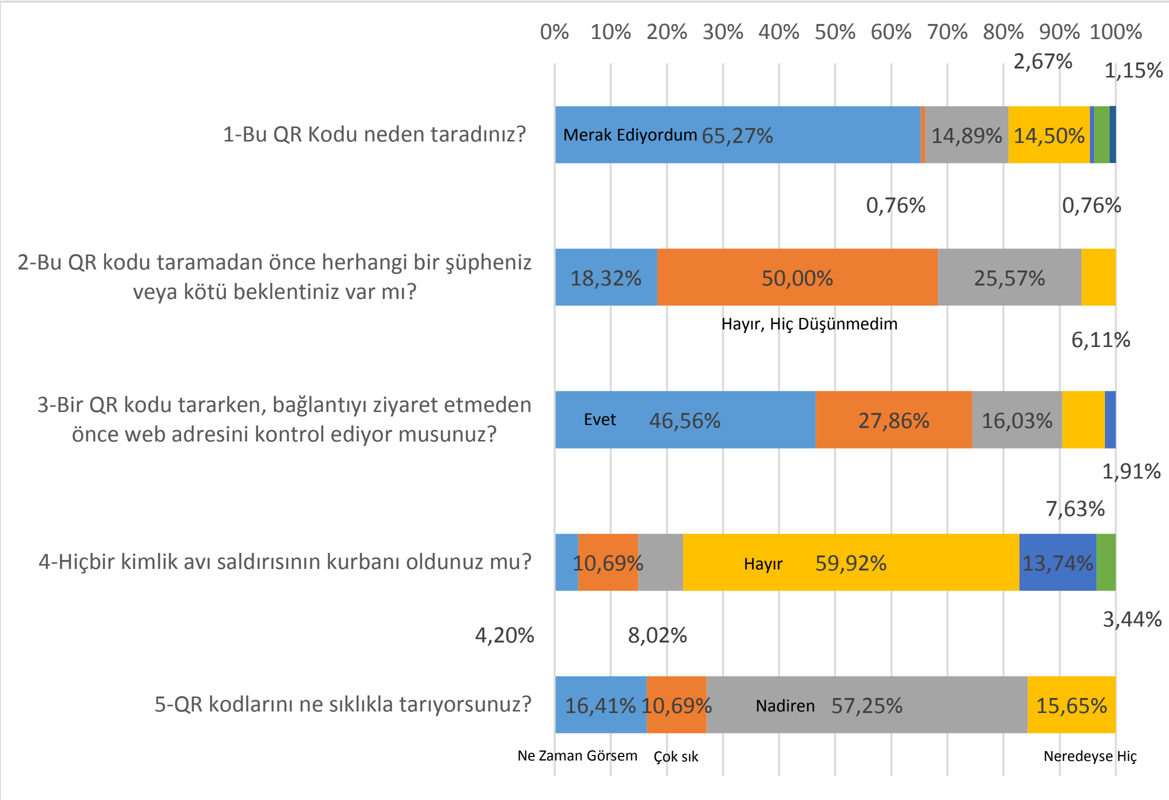
Anketimize katılan katılımcıların, sade QR Kod, talimatlı QR Kod ve Resimli QR Kod afişlerindeki cevaplar dahil olmak üzere toplamda 262 adet anket cevaplanmıştır. Şekil 29'da görüldüğü üzere, üç afişin verileri birleştirilerek resim veya tanım fark etmeksizin QR Koda olan genel tutum ölçülmeye çalışılmıştır.

İlk soruda, "Merak Ediyordum" olan ilk şık 171 kişi (%65,27) tarafından cevaplanmıştır. İlgili bilgi beni çekti" olan 2. şık 2 kişi (%0,76) tarafından cevaplanmıştır. 3.Şık olan "resim ilgimi çekti" 39 kişi (%14,89) tarafından yanıtlanmıştır. 4.Şık "Sıkılmıştım" 38 kişi (%14,50) tarafından yanıtlanmıştır. 5.Şık "QR Kodun Ne olduğunu bilmiyorum" 2 kişi (%0,76) tarafından yanıtlanmıştır. 6.şık "Cevap vermek istemiyorum" 7 kişi (%2,67) tarafından yanıtlanmıştır. Son şık ise, "Diğer:…" 3 kişi (%1,15) tarafından yanıtlanmıştır. Görüleceği üzere en yüksek yanıtlanan şık "merak ediyordum" olmuştur.

İkinci soruda, 1.şık olan "Hayır her şeyin güvenilir olduğunu düşündüm" 48 kişi (%18,32) tarafından yanıtlanmıştır. 2.şık olan "Hayır, hiç düşünmedim" 131 kişi (%50) tarafından cevaplanmıştır. 3.şık "Evet biraz garip görünüyordu" 67 kişi (%25,57) tarafından yanıtlanmıştır. 4.şık "Evet, her zaman şüpheliyim" 16 kişi (%6,11) tarafından yanıtlanmıştır. Soruya gelen en yüksek cevap sayısı görüleceği üzere %50'lik kısımla şüphe veya kötü beklenti üzerine hiç düşünmemiştir.

Üçüncü Soruda, 1.şık olarak web adreslerini kontrolünü yapan kişi sayısı 122'dir (%46,56). 2.şık olan kontrol etmeyip bağlantıyı otomatik ziyaret eden kişi sayısı 73'dür (%27,86). 3.şık "Hayır" Cevabıyla hiç kontrol etmeyen kişi sayısı 42'dir (%16,03). 4.şık web adreslerini nasıl kontrol edebileceğini bilmeyen kişi sayısı 20'dir (%7,63). 5.şık web adreslerini kontrol edip etmediğini hatırlamayan kişi sayısı 5 kişidir (%1,91).

Dördüncü Soruda, kimlik avı saldırısı kurbanı olan 11 kişidir (%4,20). Emin olamayan 28 kişidir (%10,69). "Hayır, ama tanıdığımızın başına geldi" cevabı veren 21 kişidir (%8,02). Kimlik avı saldırısına uğramayan 157 kişidir (%59,92). Kimlik avı saldırısı hakkında bilgi sahibi olmayan kişi sayısı 36'dır (%13,74). Cevap vermek istemeyenler ise 9 kişidir (%3,44). Daha önce kimlik avı saldırısına uğramayan kişiler çoğunluktadır.

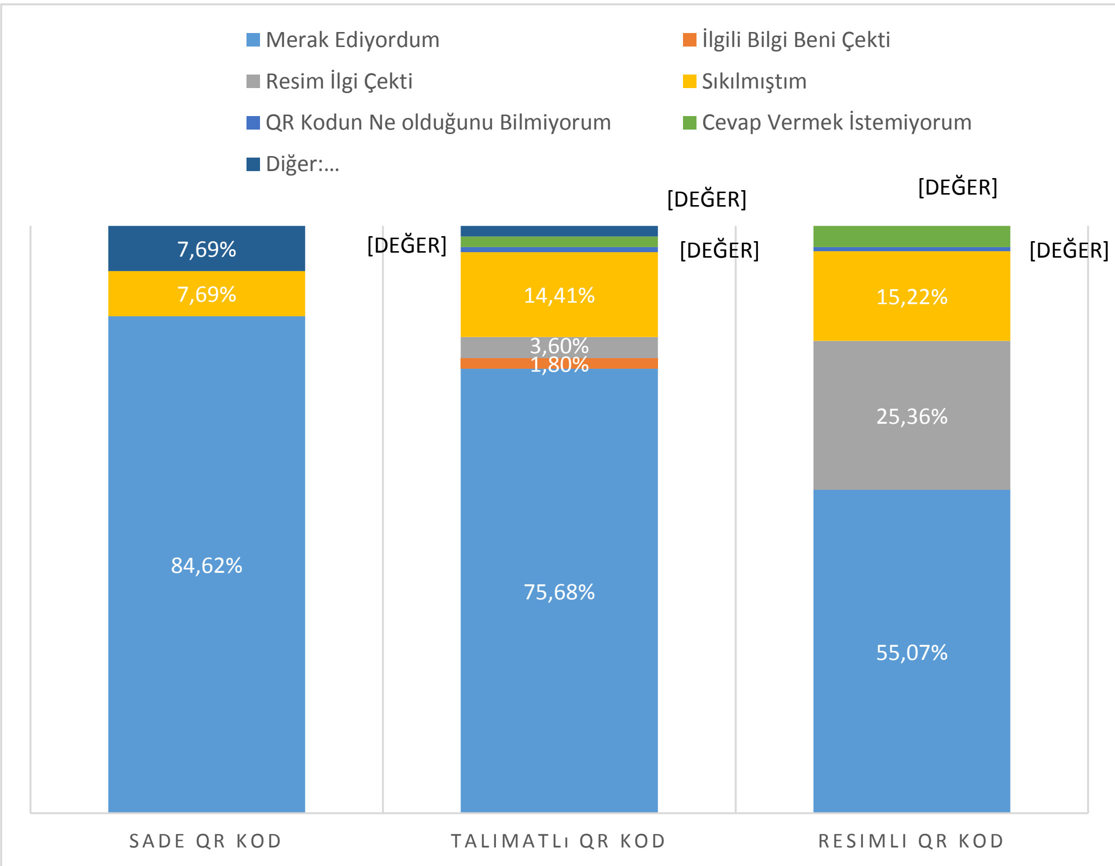


Şekil 29. QR Kod Afişlerine Verilen Cevapların Toplamı ve Analizi

Beşinci Soruda, Ne zaman görsem tararım seçeneğini seçen kişi sayısı 43'dür (%16,41). Çok sık tarayanlar 28 kişidir (%10,69). Nadiren tarayanlar 150 kişidir (%57,25). QR Kodu Neredeyse Hiç taradıklarının yanıtı verenler ise 41 kişidir (%15,65).

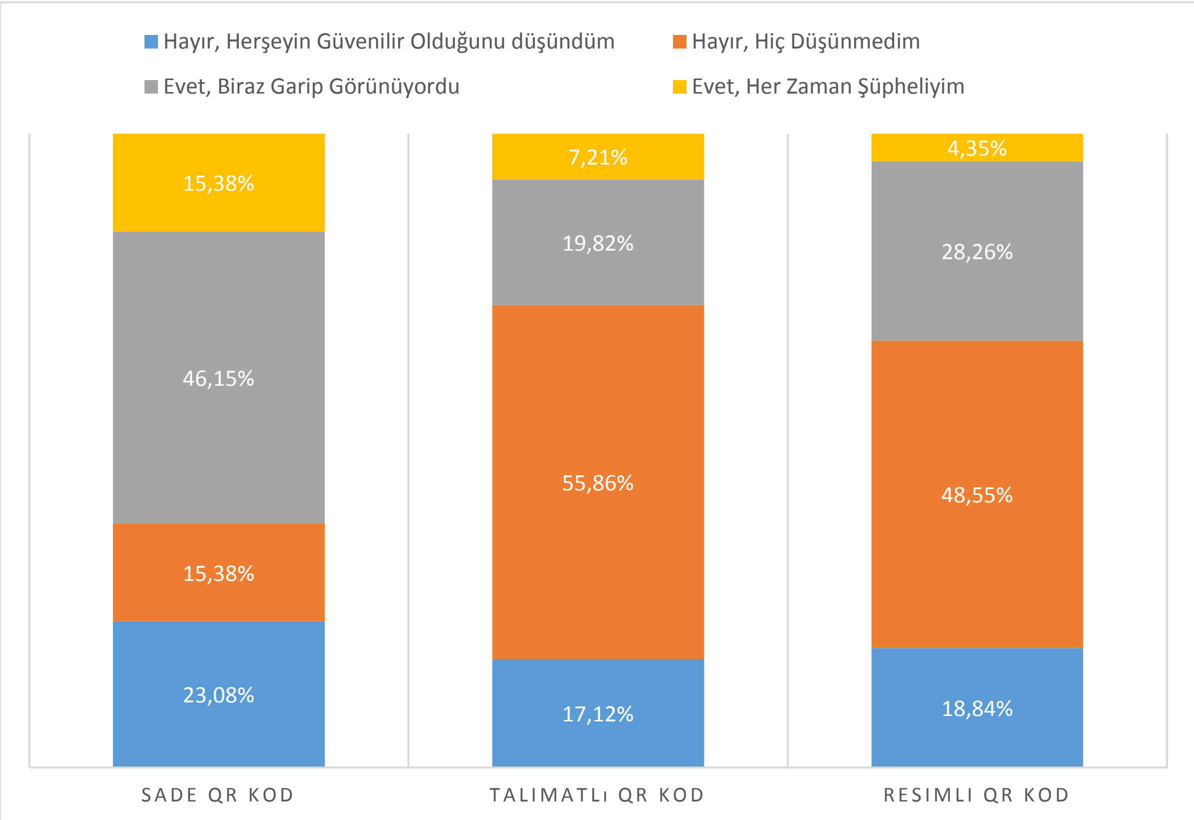
5.5. QR Kodlar Arası Karşılaştırma Analizi

İlk Soru olan “Bu QR Kodu neden taradınız?” sorusu Şekil 30’da görüldüğü üzere tüm QR Kod afişlerinde merak edildiğinden dolayı en yüksek orana sahiptir. Sade QR Kod afişinde sadece QR Kod bulunması insanlar tarafından merak uyandırmıştır. Talimatlı QR Kod afişinde ise, QR Kod dışında resim bulunmamasına rağmen “Resim ilgimi çekti” seçeneğinin seçilmesinden merak duygusunun yarattığı istek sonucu olduğu şekilde yorumlanabilir. Diğer afişlere oranla en yüksek anket cevap sayısı ve tıklanma oranı bulunan Resimli QR Kod afişlerinde ise, “Resim ilgimi çekti” %25,36 seçilmiştir. “Resim ilgimi çekti” cevabı “Merak Ediyordum” cevabından oran olarak daha düşük olmasının nedeni şıklarda “Merak Ediyordum” seçeneği önce geldiği için olabilir. Diğer taraftan “Resim ilgimi çekti” cevabı da aslında merak duygusunu içinde barındırmaktadır. Toplamda “QR Kodun ne olduğunu bilmiyorum” seçenekleri az sayıda işaretlenmiştir. Bunun sebebi QR Kodun günlük yaşantımıza adapte olmaya başladığının göstergesi olarak yorumlanabilir.



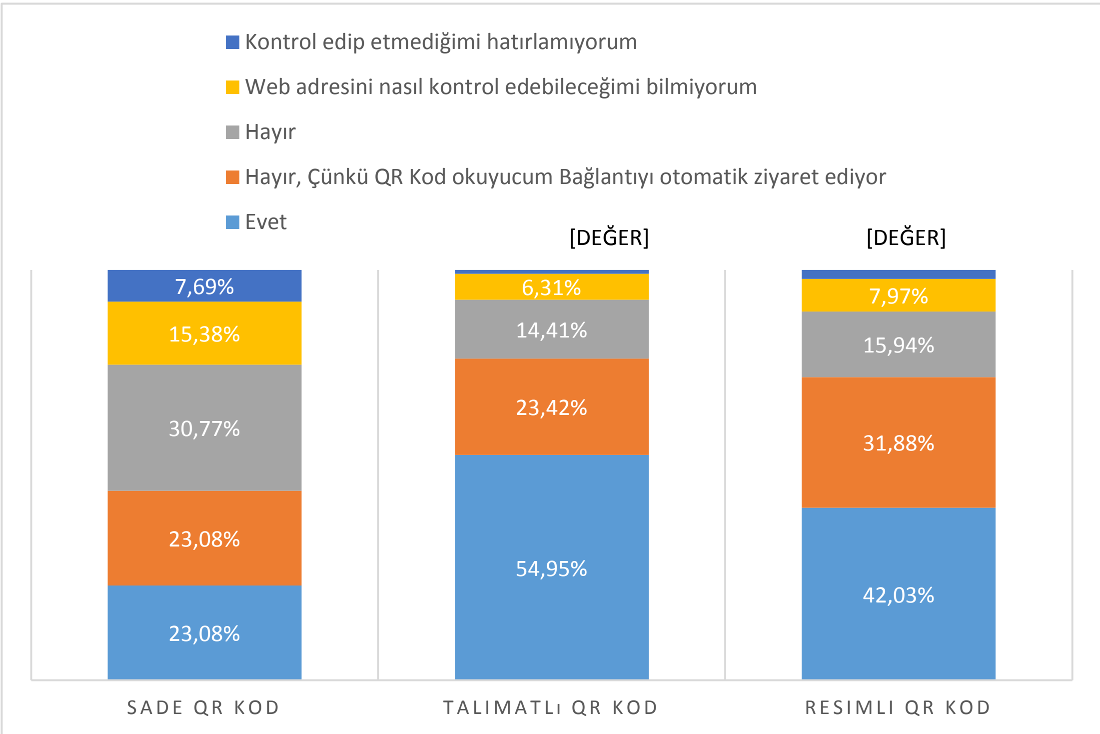
Şekil 30. Birinci Soru Cevaplanma Grafiği

Şekil 31'de görüldüğü üzere, ikinci soruda QR Kodu taramadan önce herhangi bir şüpheniz veya kötü bir beklentiniz var mı? sorusu sorulmuştur. Her şeyin güvenilir olduğunu düşünen katılımcıların Sade QR Kodda diğerlerine göre oranın fazla olması, sadece QR Kod çıktısının insanlara daha masum geldiği şeklinde yorumlanabilir. Böylece bir saldırı yapılacağının ihtimalinin olma olasılığı insanlar tarafından daha düşük algılanmış olabilir. Aynı zamanda QR Koddan gelebilecek tehlikelere karşı farkında olmadıklarını göstermektedir. "Hayır, hiç düşünmedim" seçenek oranları talimatlı ve resimli QR Kod afişlerinde fazla olduğu gözükmektedir. QR Kodun nereye yönlendirdiğini bilmeden resimler ve yazıya güvenerek tehlikeli olabileceği düşünülmemiştir. "Evet, biraz garip görünüyordu" seçeneği ise sade QR Kodda tek başına yüksek olmasının nedeni, QR Kod çıplak gözle okunamadığı için ve kodun neyle ilgili olduğu yani altında herhangi bir bilgilendirmenin veya resmin olmamasıdır.



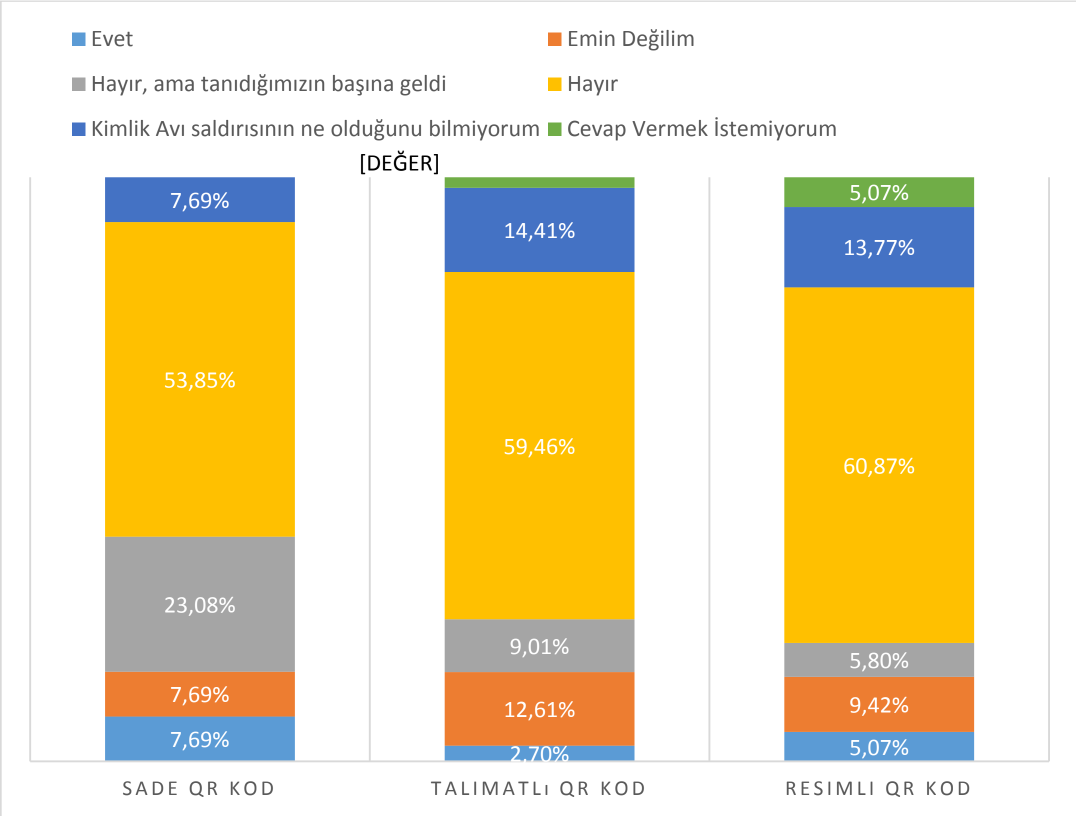
Şekil 31. İkinci Soru Cevaplanma Grafiği

Üçüncü soruda, katılımcılara QR Kodu tararken, bağlantıyı ziyaret etmeden önce web adresini kontrol edip etmedikleri sorulmuştur. Daha önce bahsedildiği gibi, interneti kullanan kişiler için URL kontrolü temel güvenlik önlemlerinden birisidir. Linki ziyaret etmeden önce kontrol yapan kişilerin oranı talimatlı ve resimli olanda sade QR Koda göre daha fazladır. Kontrol edip etmediğini hatırlamayan kişi sayısı oldukça düşüktür. Kontrol etmeyen kişilerin Sade QR Kodda fazla olmasının nedeni, diğer QR Kodlardaki resim veya talimatın bir ön bilgi oluşturup merak duygusunu arttırdığı şeklinde yorumlanabilir. Dolayısıyla katılımcının, hangi bağlantıya yönlendirildiğini kontrol etme oranı artmıştır. Şekil 32'de üçüncü soru cevaplanma grafiği yer almaktadır.



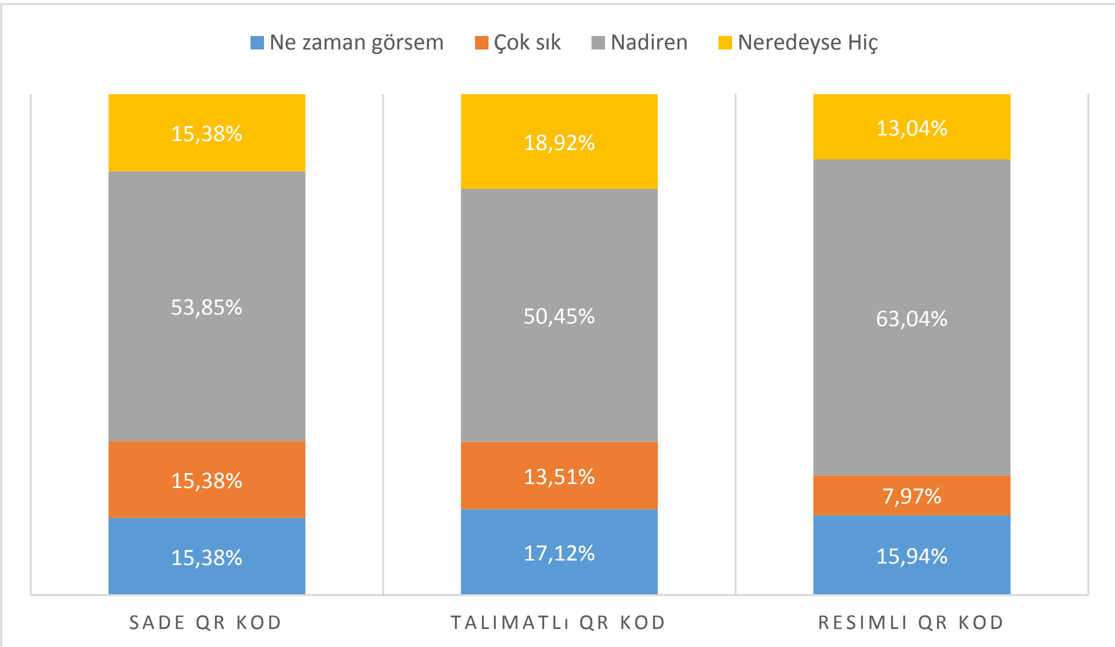
Şekil 32. Üçüncü Soru Cevaplanma Grafiği

Dördüncü soruda insanlara kimlik avı saldırısına uğrayıp uğramadıkları sorulmuştur. Sade QR Kodda "Evet" cevabını veren kişiler sade QR Kodun daha masum ve zarar gelmeyeceği düşüncesiyle hareket etmiş olabilecekleri şekilde yorumlanabileceği için oranı fazladır. "Hayır, ama tanıdığımızın başına geldi" cevabı da aynı şekilde burada yüksek oran almıştır. Aynı zamanda kimlik avı saldırısına uğramadıklarını söyleyen katılımcı oranları da tüm cevaplardan daha yüksektir. Şekil 33'te dördüncü soru cevaplanma grafiği yer almaktadır.



Şekil 33. Dördüncü Soru Cevaplanma Grafiği

Beşinci soruda QR Kodları tarama sıklık dereceleri sorulmuştur. En yüksek orana sahip cevap nadiren olmuştur. Şekil 34'te beşinci soru cevaplanma grafiği yer almaktadır.



Şekil 34. Beşinci Soru Cevaplanma Grafiği

VI. SONUÇ VE DEĞERLENDİRME

Bu çalışmada Kapsalis 'in (2013) tartışma sıralaması model alınmıştır. Kapsalis, QR Kodların kullanımına ilişkin 5 tartışma konusu belirlemiştir. Benzer şekilde bu çalışmanın bulguları, Kapsalis'in tartışma konuları baz alınarak değerlendirilmiştir. Bu tartışma konuları, giriş bölümünde belirtilen araştırma sorumuzun da cevaplanmasına yardımcı olacaktır.

QR Kod, birçok farklı alanda kullanılan ve hızla gelişen bir teknolojidir. QR Kod, farklı alanlardan gelen gereksinime göre avantaj ve kolaylıklar sunmaktadır. Reklam, pazarlama, eğitim gibi birçok alanda kullanılmaktadır. Ayrıca, son zamanlarda bankalarda para çekme vb. işlemler ile QR Kod kullanarak ödeme yöntemlerinde yeni hizmetler ortaya çıkmıştır. Bu gelişmeler ile birlikte güvenlik endişeleri ortaya çıkmaktadır. QR Kod güvenliği, kişilerin maddi veya manevi olarak zarar görmemesi açısından önem taşımaktadır. Kötü niyetli kişiler tarafından düzenlenebilecek saldırılarda, kullanıcı, parola, kredi kartı bilgileri vb. gizli ve hassas bilgilerin ele geçirilmesiyle kullanıcıların beklenmeyen bir maliyet ile karşılaşmaları mümkündür. Bu çalışmada QR Kodların saldırı amaçlı kullanıldığı kimlik avı saldırılarına (Phishing) odaklanılmıştır. Ayrıca bu çalışma kullanıcıların QR Kod güvenlik farkındalığı konusundaki bilgi ve seviye düzeylerinin tespit edilmesine yardımcı olmuştur.

6.1. QR Kodlar ile İlgili Karşılaşılabilecek Güvenlik Sorunları

Bu çalışma, QR Kodların, kimlik avı saldırısını gerçekleştirme aracı olarak nasıl kolayca kullanılabileceğini göstermektedir. Yasal olan web siteleri maskelenerek, insanların kullanıcı adları, şifreler, kredi kartı bilgileri gibi hassas bilgiler kötü niyetli kişiler tarafından ele geçirilme tehlikesi bulunmaktadır. Saldırı tipleri çok çeşitli olabilmektedir. SQL ve komut enjeksiyonu, XSS tarayıcı tabanlı saldırılar kötü niyetli kişiler tarafından uygulanabilmektedir. QR Kod ile ödeme yöntemlerinde dolandırıcılık ve sahtekarlık yapılabilmektedir. Saldırgan tarafından orijinal QR Kod manipüle edilerek, sahte bir QR Kod yapılarak saldırı düzenlenebilmektedir. Bölüm 1.2' de bahsedildiği gibi Paypal, Tek tık ile ödeme yöntemini bazı ülkelerde devreye sokmuştur. QR Kodu tara ve öde sistemi kolaylıklar sağlayabileceği gibi, saldırganlar tarafından kötüye de kullanılabilmektedir. Paypal ile yapılan ödemelerde genellikle ödemenin alıcısının kullanıcı adı girilmektedir. Saldırgan QR Kodundaki alıcının adını değiştirebilmektedir. Meşru birine çok yakın bir kullanıcı adı kullanmak, saldırganın müşteriyi fark etmeden ödemelerini hesabına yönlendirmesini kolaylaştıracaktır. Özellikle de yardım kampanyaları, yarışmalar gibi halka açık düzenlenen kampanyalardaki posterlerde veya afişlerde bulunan QR Kodlarını değiştirebilmekte ve bu şekilde kimlik avı saldırısı yapılabilmektedir. Saldırgan, ödenecek olan ücreti kendi hesabına yönlendirebilmektedir. Şu anda, bankaların çoğunluğu müşterilerine, QR kodlarını otomatik olarak okuyan ve ödeme transferlerine dönüştüren akıllı telefonlar için bir eBanking uygulaması (internet bankacılığı uygulaması) sunmaktadır. QR Kod ile ödeme yönteminin güvenli hale getirilmesi için, ödeme transferlerinin gerçekleşmesi ve alacaklı tarafından güvenli bir şekilde tahsis edilmesi için bir standart yayınlanmıştır. Ayrıca transferlerdeki kaybı da ortadan kaldıran bu sistem "Stuzza" tarafından önerilmiştir (Stuzza.at, 2019).

Bu çalışmadaki sonuçlar analiz edilirken Mobil cihazların işletim sistemleri ve versiyonları da incelenmiştir. Mobil cihazlarda toplamda %74,2 oranda en çok IOS işletim sisteminden giriş yapılmıştır. Android işletim sisteminden giriş yapan kullanıcı oranı ise %25,8'dir. Google Analitik verilerine göre, katılımcılar arasında IOS işletim sisteminde, kullanılan en güncel versiyon 13.1.3 ve en düşük versiyon 10.3.3 olarak tespit edilmiştir. Android işletim sisteminde ise, en düşük 5.0 (Lollipop) ile en güncel Android 10 (One UI 2.0 tabanlı) kullanıldığı gözlemlenmiştir. İşletim sistemi sürümleri arasında oldukça fark olduğu gözükmektedir. Bu çalışmada 11 farklı IOS versiyonu ve 47 farklı Android versiyonu tespit edilmiştir. 30 farklı web tarayıcısı sürümü tespit edilmiştir.

"eGobbler" saldırgan grubu tarafından kötü amaçlı pop-up reklamlar göstermek ve kullanıcıları kötü niyetli web sitelerine yönlendirmeye zorlamak için tarayıcı güvenlik açığından yararlanan saldırılar yapmaktadır. "eGobbler", kullanıcıları kötü amaçlı sitelere yönlendirmek için WebKit açığını kullanmıştır. Web tarayıcılardaki, web sayfalarının işlenmesine izin vermek için tasarlanan yerleşim motoru Webkit (Webkit.org) Apple'ın işletim sisteminde kullanılan uygulamalar (örn:ReplayKit API) ile birlikte güvenlik açıklarının olduğu ortaya çıkmıştır. Bu açıklar yüzünden kötü amaçlar için oluşturulmuş bir web içeriği açmak, saldırganın rastgele bir kod yürütmesine (Remote Code Evaluation zafiyeti), hassas kullanıcı bilgilerinin deşifre olmasına veya cihaza çapraz site komut dosyası (Cross-Site Scripting/XSS) saldırılarına izin verebilmektedir. Bu güvenlik açıkları, bir kullanıcının kötü niyetli bir web sayfasını ziyaret etmesini sağlayabilmekte ve saldırgan tarafından kullanılabilmektedir. QR Kod, bu tip durumlarda kullanıcıları cezbetmek amacıyla birlikte kullanılabileceği için uygun bir araçtır. Başarılı bir saldırıda, saldırganın, tarayıcının da sahip olduğu kaynaklara erişmesine neden olabilmektedir. Bu şekilde yapılan ve çerezleri çalma, oturum ele geçirme ve XSS saldırıları gibi cihazın kontrolünü ele geçirmesine neden olabilecek birçok saldırı türü mevcuttur.

6.2. QR Koduna Saldırmak

Bu çalışmada, bir QR Koduna saldırmanın mümkün olup olmadığını görebilmek için II. Bölümde çeşitli saldırı yöntemleri ve gerçekleştirilen saldırılardan bahsedilmiştir. Saldırgan, orijinal QR Kodu manipüle edip, zararlı QR Kod yaratabilmektedir. Renk değişimi ve modülleri ile oynanabilmektedir. Bu şekilde QR Kodun yönlendirdiği URL değiştirebilmektedir. Yeni saldırgan bir QR Kod üretilip, orijinal Kodun üstüne çıkartma şeklinde yapıştırılabilmektedir. Ancak bu yöntem zaman aldığı için çoğu saldırgan tarafından tercih edilmese de bu şekilde saldırı yapılması mümkündür.

6.3. Kimlik Avı Saldırılarında Saldırı Vektörü Olarak QR Kod Kullanımı

Bu çalışmada, QR Kodlarını kullanarak bir kimlik avı saldırısının uygulanabilirliğini belirleyecek şekilde tasarlanmış ve yerleştirilmiştir. Sonuçlara göre, böyle bir saldırının gerçekleştirilmesinin mümkün olduğu ve büyük olasılıkla başarılı bir şekilde gerçekleştirildiğini göstermektedir. 834 kişinin QR Kod afişlerinin yönlendirdiği web adresini ziyaret ettiği ve 262 kişinin anketi cevapladığı görülmektedir. Bu durum, QR Kodların taratıldığı ve web sayfasını ziyaret ettikleri gerçeği böyle bir saldırı senaryosunu mümkün kılmaktadır. İçeriği hakkında bilgi vermeyen ve bilinmeyen rastgele bir QR Kodun taranma oranı oldukça yüksektir. Bu tip saldırılarda, saldırganın ne kadar başarılı olacağı belirsizdir. Kurbanın, değerli bilgileri çalınabilmektedir. Saldırının başarısı web sitesinin ne kadar profesyonel olduğuna bağlı olarak, kurbanın zararlı web sayfasını ziyaret etmesine bağlıdır.

Mevcut QR Kodlarını gizlemek veya sahte reklam kullanmak gibi bir saldırganın izleyebileceği başka tekniklerle bir kimlik avı saldırısının etkinliği ve başarısını önemli ölçüde arttırabilmektedir. Bunun yanı sıra saldırgan, bir QR Kodunu yenisiyle örtebilmektedir. Kullanıcılar bu durumu fark edebildiği için saldırıdan kaçınma olanakları bulunmaktadır. Her durumda, bu saldırı teknikleri geliştikçe gelecekte tekrar bir araştırmanın konusu olacaktır.

Ankete katılım sağlayan kişi sayısının 262 olmasına rağmen tüm web sitesi trafiğe bakıldığında, toplamda 834 kişinin web adresini ziyaret ettiği tespit edilmiştir. Bu durum da anket formunu doldurmanın aslında daha önemsiz olduğu ve 834 kişinin avlandığını göstermektedir.

6.4. QR Kodlarıyla İlgili Tehditlere İlişkin Güvenlik Farkındalığı Seviyesi

Kullanıcıların güvenlik farkındalığı seviyesini belirlemek için, çevrimiçi anketten alınan cevaplar incelenmiştir. Cevap olarak kimlik avı saldırısının ne olduğunu bilmiyorum ve emin değilim cevabını seçen katılımcı oranı düşüktür. Buradan katılımcıların çoğu kimlik avı saldırısı hakkında bilgili olduğu düşünülebilir. Kimlik avı saldırısına hiç uğramayan yani hayır cevabını verenler en yüksek çoğunluktadır. Tanıdıklarının başına gelen olaylar, gazete, televizyon veya kamu spotu gibi yerlerden bilgi edinmiş olabilirler. Fakat bütün bunlar kullanıcıların kendilerini nasıl koruyacaklarını bildikleri anlamına gelmemektedir. Kullanıcılar çoğunluk olarak URL’yi kontrol ettiklerini, zararlı olabileceği hakkında hiç düşünmediklerini bildirmiştir. Her ne kadar URL olarak Başkent Üniversitesi alan adı kullanımı katılımcılara güven vermiş olsa da profesyonelce hazırlanmış bir site URL’sinde saldırgan başarılı olabilir. Buradan, kullanıcıların, kimlik avı saldırısının ne olduğu hakkında teorik bir anlayışa sahip olabileceği ve fakat genel olarak böyle bir saldırının hedefi olabileceği sonucuna varmaktadır. Bununla birlikte, bilgilerini pratikte uygulayamayabilir ve kendilerini koruyamayabilirler. Ayrıca olası tehditlerin farkında olsalar bile, onlarla başa çıkacak uygun becerilere sahip olmayabilirler. Uygun güvenlik göstergelerini sağlayan etkili mobil güvenlik yazılımı gibi teknik araçların bulunmaması bu durumu daha da zorlaştırmaktadır. Ayrıca, üçüncü soruda katılımcılar (%27,86) QR Kod okuyucum bağlantıyı otomatik ziyaret ediyor cevabını vermiştir. Otomasyona duyulan güven, güvenlik bilinci oluşturmada ciddi bir engeldir.

6.5. QR Koduna İlişkin Güvenlik Sorunlarına Karşı Alınabilecek Önlemler

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) Bu tip güvenlik uygulamaları; antivirüs, fidye yazılımı koruması, mobil güvenlik, parola yönetimi, VPN ve ebeveyn denetimlerini içermektedir.

Temel güvenlik önlemi, QR Kod okuyucuların izlemesi gereken bir güvenlik çerçevesi oluşturmaktadır. Bazı kişiler bağlantıyı otomatik ziyaret ettiklerini bildirmişlerdir. Bağlantıyı ziyaret etmeden önce URL’yi manuel olarak kontrol etmek, en basit fakat aynı zamanda bir kullanıcının gerçekleştirebileceği en temel güvenlik kontrolüdür. Daha önce de bahsedildiği gibi, ziyaret etmeden önce URL’yi kontrol etmeyi sağlayan bir QR Kod yazılımına sahip olmak, kullanıcıya ziyaret etmek üzere olduğu URL’nin reklamı yapılan ile aynı olduğunu doğrulama yeteneği vermektedir. Yanında herhangi bir bilgi bulunmayan QR Kodlarında bu güvenlik kontrolü mümkün değildir. Bu nedenle, tüm QR Kod okuyucuları, 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 okuyucusuna gömülebilmektedir. Örneğin, bir kullanıcı kendisini geçerli bir sertifikası olmayan veya güvenli olmayan bir bağlantı kurmaya çalışan bir web sayfasına yönlendiren bir QR Kodunu taradığında, okuyucu kullanıcıyı bilgilendirmelidir. Yeni çıkan mobil cihazlarda, kamera uygulamasında QR Kod okumak için ayar bulunmaktadır. Bu basit ayar aktifleştirildiğinde, kişisel fotoğraf ve video için kullandığımız cihazın kendine ait olan kamerasından QR Kod tarama özelliği aktif olmaktadır. Ayrıca burada QR Kodu tarattığınız anda, “URL’ye gitmek için bildirime tıklayın” bildirimi gelmekte ve URL gözükmektedir. Yeni bir mobil cihazda, alınan markanın özelliğine göre bu durum değişebilir. Eğer bu tür bir özellik varsa ek olarak yeni bir QR Kod okuyucu indirilmesi gerekmemektedir.

QR Kodunun yayıncısı tarafından oluşturulan ve kodlanan içeriğe eşlik eden dijital imza, kodlanan bilgilerin bütünlüğünü doğrulayabilmektedir. Bunu başarmak için, QR Kod okuyucu, dijital imzayı orijinal yayıncıyla eşleştirebileceği, doğrulanmış bir veri tabanına erişebilmelidir. İmza bilinen yayıncıların hiçbiriyle eşleşmiyorsa, QR Kod okuyucusu kullanıcıya bir güvenlik bildirimi gösterebilir ve bağlantıyı ziyaret edip etmemek için nihai kararı kullanıcıya bırakabilir. Bu çözüm, QR Kodlarının çalışmasını biraz zorlaştırabilir ve dijital imza, QR Kodun kapasitesinin bir bölümünü tüketmektedir. Ayrıca, bir web sitesinin SSL sertifikasının bulunması tamamen güvenli olduğu anlamına gelmez ancak SSL sertifikasının bulunması kullanıcı tarafından güveni arttırmaktadır.

Kullanıcıların eğitilmesi, güvenlik sorunlarının üstesinden gelmenin en etkili ve aynı zamanda en zor yoludur. Öncelikle, kullanıcılar bağlantıyı ziyaret etmeden önce URL’yi her zaman kontrol edecek şekilde eğitilmelidir. Rastgele bir QR Kodunu taramanın ve karşılık gelen URL'yi ziyaret etmenin, belirsiz ve bilinmeyen bir etki alanını ziyaret etmekle tamamen aynı olduğunu fark etmek son derece önemlidir. Kullanıcılar, kodu çözülmüş URL'nin, ilgili poster veya afişin reklamını yapan ile aynı olup olmadığını kontrol etmek için eğitilmelidir. QR Kodun yakınında yönlendirdiği yer ile ilgili bir bilgi yoksa, kullanıcı çok dikkatli olmalı ve devam etmenin kötü niyetli bir web sayfasını ziyaret etmek anlamına gelebileceğinin farkında olmalıdır. Bununla birlikte, kullanıcıları eğitmek her zaman pahalı ve zaman alan bir süreçtir. Kullanıcılar otomatikleştirilmiş özelliklere daha fazla güvenme eğilimindedirler ve zamanlarını uygun teknik eğitim almak için harcamak istemezler. Ayrıca, bir URL’nin yalnızca ona bakarak kötü amaçlı olduğunu doğrulamak oldukça zor bir iştir. Bu nedenle, kullanıcıların eğitiminde; gizli URL’leri ziyaret etmekten kaçınılmalı ve doğrulanmamış kaynaklara hassas ve kişisel bilgiler vermemeye odaklanılmalıdır.

Son olarak, bu çalışmada, toplumsal yaşamda bireylerin QR Kodların olası güvenlik zafiyetleri ve yarattığı güvenlik sorunları ile bu konu hakkındaki kullanıcıların farkındalık seviyeleri araştırılmıştır. Bir sosyal mühendislik deneyi olarak bakıldığında bu çalışma, QR Kodlar ile ilgili güvenlik konularında kullanıcıların güvenlik farkındalığı düzeyini belirlemek amacıyla hedefine ulaşmıştır. Farklı yerlere yerleştirilen QR Kod afişleri ile 262 ziyaretçinin ankete katılımı sağlanmıştır. QR kod afişinin yönlendirdiği web adresinin tıklanma sayısı ise 834 kişidir. Bu yöntemle yapılabilecek olası bir kimlik avı saldırısının başarılı olacağı sonucuna ulaşılmıştır. Aynı zamanda, katılımcıların çoğunun Şüpheleri olsa bile bir QR Kodunun nereye yönlendirdiğini keşfetmeye meraklı olduğu görülmüştür. Kimlik avı saldırılarında QR Kod kullanımının çok yaygın olmaması bu alanda farkındalık seviyesini de düşürmektedir. Farkındalığın düşük olması ise saldırganların bu tür saldırılardan başarı elde etmesini kolaylaştırmaktadır. Gelişen teknolojiyle birlikte QR Kodlar daha sık kullanılmaya başlayınca yeni yöntemler geliştirilebilir.

Sonuç olarak, Ankara ilinde yapılan bu çalışmada katılımcıların QR Kod güvenlik farkındalığının düşük olduğu gözlemlenmiştir. Farkındalığın arttırılması için kullanıcı eğitimi son derece önemlidir. Ek olarak, kullanılan akıllı mobil cihazın web tarayıcısı ve işletim sisteminin güncel versiyonlarının yüklenmesi güvenli QR Kod okuyucusu ve çeşitli güvenlik uygulamaları kullanımı güvenlik seviyesini arttırmada etkili olacaktır.

KAYNAKLAR

Acartürk, C. (2012). *Barkod Teknolojilerinin Eğitimde Kullanımı: Bilişsel Bilimler Çerçevesinde bir Değerlendirme.* Akademik Bilişim’12 - XIV. Akademik Bilişim Konferansı Bildirileri, Uşak Üniversitesi, 117.

Ahuja, S. (2014). *QR Codes And Security Concerns.* (IJCSIT) International Journal of Computer Science and Information Technologies, 5 (3), 3878.

Akyazı, E. (1994). *Barkod Teknolojisi ve Barkod Üretim Teknikleri.* Marmara İletişim Dergisi, Sayı 7, 146-147.

Al-Khalifa, H. S. (2008). *Utilizing QR Code and Mobile Phones For Blinds And Visually Impaired People, K. Miesenberger et al.* (Eds.): ICCHP 2008, LNCS 5105, 1065-1069.

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

Android Market Google Play Store-a, Kaspersky Lab, (2019). https://play.google.com/store/apps/details?id=com.kaspersky.qrscanner 10.10.2019 tarihinde erişildi.

Android Market Google Play Store-b, Trend Micro, (2019). https://play.google.com/store/apps/details?id=com.trendmicro.qrscan&hl=en 10.10.2019 tarihinde erişildi.

Arslan, D., Atasever, V., Güvenoğlu, E. Ve Erdoğan, Ş. (2010). *Çizgi Barkod Sistemleri ve HCCB Barkod Sisteminin Karşılaştırılması.* Akademik Bilşim’10 – XII. Akademik Bilişim Konferansı Bildirileri, 394.

Arslan, M. (2011). *Kare Kodlar ile Hayatımız Değişecek!.* Tübitak Bilim ve Teknik Dergisi, 44(523), Haziran, 78-79.

Bani-Hani, R. M. Wahsheh, Y. A. Al-Sarhan, M. B. (2014). *Secure QR Code System.* 10th International Conference on Innovations in Information Technology (IIT). 2. DOI: 10.1109/INNOVATIONS.2014.6985772

Başkent Üniversitesi, (2019). http://angora.baskent.edu.tr/bilgipaketi/ 30.12.2019 tarihinde erişildi.

Bayrak Meydanoğlu, E. S. Ve Klein, M. (2015). *Türk Tüketicisinin QR Kod Kullanımı Üzerine Keşfedici Bir Araştırma,* Akademik Sosyal Araştırmalar Dergisi, 3 (19), 48.

Bayram, U. Ve Çetinkaya, V. (2007). *Kütüphane Otomasyonu. IV. Otomasyon Sempozyumu*, 23-25 Mayıs 2007 TMMOB (Samsun) ve Ondokuz Mayıs Üniversitesi, Samsun-Türkiye, 69.

Bilici, F. (2015). *Pazarlamada Artırılmış Gerçeklik ve Karekod Teknolojileri: Tüketicilerin Artırılmış Gerçeklik Teknoloji Algılamaları Üzerine Bir Alan Araştırması*, 96-102.

Chu, H. K. Chang, C. S., Lee, R. R., Mitra, N. J. (2013). *Halfttone QR Codes. ACM Transactions on Graphics*, vol 32 (6), Article 217, 1-8.

CSO From IDG Communications, https://www.cso.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-malicious-qr-codes/ 17.10.2019 tarihinde erişildi.

CSO From IDG, *AVG (AU/NZ) Cautions: Beware of Malicious QR Codes* (Dikkat: Kötü amaçlı QR Kodlara Dikkat edin)

Çataloğlu, E. Ve Ateşkan, A. (2014). *Use of QR Codes in Education With Examples (QR Kodunun Eğitim ve Öğretimde Kullanımının Örneklenmesi).* Elementary Education Online, 13(1), 5-13.

Ceipidor, U. B., Marsico, M. Ve Romano G. (2009). *A Museum Mobile Game for Children Using QR-Codes*, 282-283.

David Ulevitch, Phistank (OpenDNS), (2006) https://www.phishtank.com/ 15.10.2019 tarihinde erişildi.

Denso Wave Incorporated, (2003). QR code.com. http://www.qrcode.com/en/ 15.10.2019 tarihinde erişildi.

Elçi, A. (2014). *İş Ekipmanlarında Güvenlik Takibi İçin Bir Sistem Önerisi "Karekod Barkod Uygulama".* 1-63.

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

Göksel B. Ve Başaran A. (2016) "QR-Code'daki Olta Bir Farkındalık Deneyi ve QR Kodların Sosyal Mühendislik Saldırılarında Kullanılması", Garnizon Bilgi Güvenliği Ltd. Rapor

Github, (2019). https://github.com/OWASP/QRLJacking 11.12.2019 tarihinde erişildi.

Hacettepe Teknokent, (2019). https://www.hacettepeteknokent.com.tr/tr/firmalar#0 30.12.2019 tarihinde erişildi.

Hendry, M. R., Rahman, M. N. A., ve Seyal, H. A. (2017). *Smart Attendance System Applying QR Code.* 12th International Conference on Latest Trends in Engineering and Technology (ICLTET'2017), 1.

Kapsalis, I. (2013). *Security of QR Codes.* Norwegian University of Science and Technology Department of Telematics, 1-75.

Kieseberg, P., Leithner, M., Mulazzani, L., Schrittwieser, S., Sinha, M., Ve Weippl, E. (2010). *QR Code Security*, 5-6. DOI: 10.1145/1971519.1971593.

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

Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Ve Weippl, E. (2014). *QR Code Security*: *A Survey of Attacks And Challenges For Usable Security*, 7-8.

Li, L., Fan, M., & Wang, G. (2018, November). LWSQR: Lightweight Secure QR Code. *In International Conference on Frontiers in Cyber Security* (pp. 241-255). Springer, Singapore.

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

Masalha, F., ve Hirzallah, N. (2014). *A Students Attendence System Using QR Code*. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, (3), 75.

Milliyet Gazetecilik ve Yayıncılık A.Ş. (2012). *Tribünde barkod pankart açanlar aranıyor.* http://www.milliyet.com.tr/skorer/tribunde-barkod-pankart-acanlar-araniyor-1496180 10.11.2019 tarihinde erişildi.

Mitnick, K.D., Simon, W.L., (2013). *“Aldatma Sanatı”*, Odtü Yayıncılık, Ankara.

Moharil, B., Ghadge, V., Gokhale, C., ve Tambvekar, P. (2012). *An Efficient Approach for Automatic Number Plate Recognition System Using Quick Response Codes.* (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5), 5108.

Numan-Al-Mobin, A. M., Meruga, J. M., Cross, M. W., Kellar J. J., ve Anagnostou D. E. (2013). *QR Code Antenna For Wireless and Security Applications*. IEEE Antennas and Propagation Society International Symposium (APSURSI), 1.

Owasp, (2019). https://www.owasp.org/index.php/Qrljacking 11.12.2019 tarihinde erişildi.

Öğütçü N., (2019). *Dijitalleşmenin Türkiye Bankacılık Sektörü Üzerindeki Etkileri*. Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı, Maltepe Üniversitesi, İstanbul. 33-44.

Örücü, A. İ. (2013). *Bir Vergi Ödeme Aracı Olarak Karekod Teknolojisi*, Maliye Dergisi, 164, 262.

Polat, Z. A. (2014). *Karekod Teknolojisinin Mesleğimizdeki Olası Kullanımları Üzerine Düşünceler.* Uzaktan Algılama ve Coğrafi Bilgi Sistemleri Sempozyumu (Uzal-CBS 2014), 3.

PCWORLD, https://www.pcworld.idg.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-malicious-qr-codes/ 11.10.2019 tarihinde erişildi.

Sanal, A. (2017). *Hizmet Sektöründe QR KOD Kullanımı ve Uygulama Alanlarının değerlendirilmesi.* (Yayınlanmamış yüksek lisans tezi), Yaşar Üniversitesi, İzmir. 34.

Sharma, V. (2012). *A Study Malicious QR Codes.* International Journal of Computational Intelligence and Information Security, 3(5). 1-5.

Shin, D. Ve Yao, H. (2013). *A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone.* Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), 49-50.

Stuzza.at, (2019). https://www.stuzza.at/en/zahlungsverkehr/qr-code.html 06.12.2019 tarihinde erişim sağlandı.

Tarjan, L., Šenk, I., Tegeltija, S., Stankovski, S. ve Ostojic, G. (2014). *A readability analysis for QR code application in a traceability system.* Computer And Electronics In Agriculture (109), 1.

Taşkın, A. C. (2012). *Orta Ölçekli Belediyelerde Kullanılabilecek Karekod Barkod Destekli Doküman Yönetim Sistemi* (Yayınlanmamış yüksek lisans tezi), Trakya Üniversitesi, Edirne, 28.

Tiwari, S. (2016). *An Introduction To QR Code Technology*. International Conference on ınformation Technology, 43.

Türkiye İş Bankası A.Ş, (2012). *İş Bankası'ndan ödeme sistemlerinde devrim yaratacak uygulama: Parakod.* https://www.isbank.com.tr/TR/hakkimizda/haberler-ve-medya/haberler/Sayfalar/haberler.aspx?start1=111&4DDCBC12-B456-4049-8BDA-FB3415CAE7E1idCol=87 02.01.2020 tarihinde erişim sağlandı.

Qianyu, J. (2014). *Exploring The Concept Of Qr Code And The Benefits Of Using QR Code For Companies*. Bachelor's Thesis School of Business and Culture Degree Programme in Business Information Technology Bachelor of Business Administration, 44-47.

Wane, A.R. ve Jamankar, S. P. (2013). *An Effective Mechanism For Ensuring Security Of QR Code.* International Journal of Advanced Research in Computer Science. 4 (6), 176-179.

Webkit https://webkit.org/ (A fast, open source web browser engine) 06.12.2019 tarihinde erişildi.

Vidas, T. Owusu, E. Wang, S. Zeng, C. Cranor, L. F. ve Christin, N. (2013). *QRishing: The Susceptibility Of Smartphone Users To QR Code Phishing Attacks*, 1-15. DOI: 10.1007/978-3-642-41320-9_4

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.

Zhang, S. Ve Yoshino, K. (2008). DWT-Based Watermarking Using QR Code, Science Journal of Kanagawa University 19, 3-6.

EKLER

EK-1 Web Sayfasına Ait Kodlar (HTML, CSS ve Google Analitik Kodları)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
  <!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-146398724-
4"></script>
<script>
 window.dataLayer = window.dataLayer || [];
 function gtag(){dataLayer.push(arguments);}
 gtag('js', new Date());

 gtag('config', 'UA-146398724-4');
</script>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title>QR Kodların Güvenlik Farkındalığı Anketi</title>
<style type="text/css" media="screen">
html, body {
position: absolute;
height: 100%;
max-height: 100%;
width: 100%;
margin: 0;
padding: 0;
}
iframe {
position: absolute;
height: 100%;
width: 100%;
border: none;
```

```
}
#container {
position: absolute;
top: 50px;
bottom: 0;
width: 100%;

}
#header {
position: absolute;
top: 0px;
height: 50px;
color: #eee;
background-color: #ccc;
width: 100%;
}
</style>

</head>

<body>

<div id="header"></div>
<div id="container">
<iframe
src="https://docs.google.com/forms/d/e/1FAIpQLSf8fUaPDvDBTdv6sJxAH1JYI_NEbnG
kpzwEKymmDuvoW1FGSQ/viewform?usp=sf_link"></iframe>      /* Bu kısımdaki link,
anket linkidir. 3 adet anket linki oluşturulduğu için, sadece link kısmı farklılık
göstermektedir. Diğer 3 linkte kullanılan kodlama, buradaki link haricinde aynıdır. */
</div>
</body>
</html>
```