

SİBER GÜVENLİK TEHDİTLERİ ÇERÇEVESİNDE QR KOD TABANLI KİMLİK AVI SALDIRILARINA KARŞI KULLANICI GÜVENLİĞİ^{*,**}

USER SECURITY AGAINST QR CODE-BASED PHISHING ATTACKS IN THE CONTEXT OF CYBERSECURITY THREATS

Araştırma Makalesi
Research Paper

Mustafa Bilgehan İMAMOĞLU^{***}

Aleyna AYAZ^{****}

Öz:

Teknolojinin hızlı gelişmesiyle birlikte QR kodlar, bilgiye hızlı erişimi nedeniyle yaygın biçimde kullanılmaktadır. Ancak bu yaygın kullanım, kötü niyetli kişiler tarafından yapılan kimlik avı (phishing) saldırıları başta olmak üzere birçok siber tehdidi de beraberinde getirmektedir. Bu çalışmada, QR kodlar aracılığı ile gerçekleştirilebilecek kimlik avı saldırılarına karşı bireylerin farkındalık düzeyleri incelenmiştir. Karadeniz Teknik Üniversitesi kampüsünde gerçekleştirilen saha çalışmasında, resimsiz ve resimli olmak üzere iki farklı türdeki QR kod afişleri öğrenci yoğunluğu olan alanlara yerleştirilmiş ve kullanıcıların QR kodları tarama motivasyonları ile kimlik avı saldırılarına yönelik farkındalıkları analiz edilmiştir. Elde edilen veriler, görsel öğelerle desteklenen afişlerin daha fazla ilgi çektiğini, katılımcıların çoğunun güvenlik konusunda yetersiz bilgiye sahip olduğunu ve merak duygusunun tarama davranışında önemli bir rol oynadığını göstermektedir.

Anahtar Kelimeler: QR Kod, Kimlik Avı, Siber Güvenlik, Sosyal Mühendislik, Kullanıcı Farkındalığı

Abstract:

With the rapid advancement of technology, QR codes have become widely used due to their ability to provide quick access to information. However, this widespread use also brings along various cybersecurity threats, particularly phishing attacks conducted by malicious actors. This study investigates individuals' awareness levels regarding phishing attacks that can be executed through QR codes. A field study was carried out on the campus of Karadeniz Technical University, where two different types of QR code posters—visual and non-visual—were placed in areas with high student traffic. The motivations behind scanning the QR codes and participants' awareness of phishing attacks were analysed. The results reveal that posters supported with visual elements attracted more attention, most participants lacked sufficient knowledge about security, and curiosity played a significant role in their scanning behaviour.

Keywords: QR Code, Phishing, Cybersecurity, Social Engineering, User Awareness

* Makale Geliş Tarihi: 10.05.2025

Makale Kabul Tarihi: 21.07.2025

** Bu çalışma, Mustafa Bilgehan İMAMOĞLU'nun danışmanlığında yürütülmekte olan, Aleyna AYAZ tarafından hazırlanan "Siber Güvenlik Tehditleri Çerçevesinde QR Kod Tabanlı Saldırıları" konulu devam eden yüksek lisans tez çalışması kapsamında hazırlanmıştır.

*** Dr. Öğr. Üyesi, Karadeniz Teknik Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, bilgehan@ktu.edu.tr, <https://orcid.org/0000-0002-3496-2959>.

**** Yüksek Lisans Öğrencisi, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Yönetim Bilişim Sistemleri, aleyna1ayaz@gmail.com, <https://orcid.org/0009-0008-6731-2902>.

GİRİŞ

Siber güvenlik (Cyber Security), bilgisayar sistemleri ve ağlarını yetkisiz erişim, veri sızıntısı, siber tehditler gibi kötü amaçlı saldırılardan korumayı hedefleyen çeşitli strateji ve önlemleri içerir. Donanım, yazılım ve verilerin güvenliğini sağlayarak hizmet kesintilerini ve bilgi ihlallerini önlemeyi amaçlar (Adedoyin & Christiansen, 2023; Firmansyah, 2024). Siber güvenlik çalışmaları, 1970’li yıllarda ortaya çıkmış, ancak 1980’lerde bilgisayar korsanlığı, kötü amaçlı yazılımlar ve siber saldırılar nedeniyle bilgisayar bilimi disiplini içinde önemli bir araştırma alanı haline gelmiştir. 1990’lı yıllarda internetin yaygın hale gelmesi, siber tehditlerin artmasına ve ağ güvenliğinin öncelikli bir konu olarak ele alınmasına neden olmuştur. 2000’li yıllarda tehditlerin giderek daha karmaşık hale gelmesi, devletleri ve uluslararası kuruluşları kapsamlı siber güvenlik stratejileri geliştirmeye yönlendirmiştir. Günümüzde siber güvenlik, farklı disiplinlerin katkısıyla sürekli gelişen bir alan olarak varlığını sürdürmektedir (Tarhan, 2022).

Günümüzde siber güvenlik tehditleri giderek artmakta ve kurumlar için önemli riskler oluşturmaktadır. İç tehditlerin ilk sırada olduğu bu listede kötü amaçlı yazılımlar (malware) ve kimlik avı saldırılarının (phishing) ardından fidye yazılımları (ransomware) ve dağıtık hizmet reddi (DDoS) saldırıları gelmektedir. Bu tehditlere karşı etkin önlemler alınması gerekmektedir. Bu kapsamda, sıfır gün açıklarının tespit edilmesi, makine öğrenimi ve yapay zeka destekli tehdit algılama sistemlerinin kullanılması, saldırı tespit ve önleme sistemleri (IDS/IPS) ile ağ güvenliğinin sağlanması ve siber tehdit istihbaratı aracılığıyla olası saldırıların önceden tespit edilmesi kritik önem taşımaktadır (Shinde vd., 2024).

QR kod (Quick Response Code), hızlı yanıt anlamına gelen, beyaz bir zemin üzerine siyah motiflerden oluşan kare şeklindeki iki boyutlu barkoddur. İki boyutlu barkodlar, geleneksel tek boyutlu barkodlara göre bilgiyi saklama ve transfer edebilme konusunda başarı oldukça geniş bir kullanım alanına sahiptir (Bilir & Özkoç, 2020).

İlk olarak 1994 yılında otomobil endüstrisinde kullanılmak üzere geliştirilen QR kod, hızlı okunabilmesi, kolay dağıtımı ve üretimi sayesinde popülerlik kazanmıştır. QR kod, Toyota grubuna bağlı Denso firması tarafından geliştirilmiş, 2000 yılında veri yapısı, teknik özellikleri ve kullanım şekli açısından ISO/IEC18004 koduyla onaylanarak uluslararası bir standart haline gelmiştir. 2010 yılında ise Denso firması, QR kodun patentini serbest kullanıma açmış ve böylece tüm dünyada QR kod teknolojisinin ücretsiz kullanılabilmesine olanak sağlamıştır (Başar, 2024).

QR kodlar, web sitesi ve e-posta adreslerinden ürün görsellerine hatta indirim kuponlarına kadar geniş bir yelpazede farklı türde bilgiyi erişilebilir kılmayı mümkün kılan bir teknolojidir (Sun vd., 2007). QR kodlar, kullanıcıları ilgi alanlarına yönelik daha fazla hizmet veya bilgi sunan web sitelerine yönlendirmek için birçok farklı alanda kullanılmaktadır. Bunlardan biri, otomatik plaka tanıma sistemlerinde, plakadaki harflerin veya sayıların okunmasında karşılaşılabilecek hatalara karşı plakalara QR kodlar eklenerek görüntü işlemedeki sorunların giderilmesidir (Moharil vd., 2012). Diğer bir uygulama ise yük asansörü, asma iskele gibi iş ekipmanlarına QR kod yerleştirilerek çalışanların ve

ekipmanların bilgilerine kolayca erişebilmesini sağlamak; böylece ekipman güvenliğini artırmak, iş kazalarını azaltmak ve sürdürülebilir güvenlik önlemleri geliştirmektir. (Elçi, 2014).

QR kod teknolojisi, çeşitli kullanım kolaylıkları ve avantajlar sağlamakla birlikte, önemli güvenlik açıklarını da beraberinde getirmektedir. Nitekim hakaret içerikli pankartların stadyumlara sokulmasının yasak olduğu bir futbol müsabakasında, Karşıyaka taraftarlarının küfür içeren bir Uniform Resource Locator (URL) adresine yönlendiren QR kodlu pankartı, Göztepe derbisinde güvenlik kontrollerini aşarak kullanabilmesi bu duruma çarpıcı bir örnek teşkil etmektedir. QR kodların çıplak gözle içeriğinin okunamaması ve yalnızca mobil veya özel cihazlar aracılığıyla erişilebilir olması, bu güvenlik zafiyetinin temel nedenlerinden biri olarak öne çıkmaktadır. Buna ek olarak, kötü niyetli kişilerin QR kodlar aracılığıyla kodu okuyan cihazların hassas bilgilerine erişim sağlaması ve bu bilgileri kötü amaçlı işlemler için kullanma riski de söz konusudur. (Bilir & Özkoç, 2020).

QR kodlar aracılığı ile yapılan saldırılarda en sık rastlanan tür sosyal mühendislik vakalarıdır. Bilgi güvenliği alanında sosyal mühendislik, bireylerin manipüle edilerek gizli bilgilerinin çalınması amacıyla bilgi hırsızlığını ifade eder. Bu yöntemlerden en çok kullanılanı kimlik avı saldırılarıdır. Kimlik avı saldırılarında, kötü niyetli saldırganlar QR kodlara zararlı URL'ler ekler ve bunları etiketler halinde hazırlayıp çeşitli nesnelerin üzerine yapııştırarak kurbanlarından kullanıcı adı ve parola gibi hassas bilgileri almak amacıyla sahte sitelere yönlendirerek dolandırıcılık amaçlarını gerçekleştirirler (Krombholz vd., 2014).

Günümüzde QR kod teknolojisinin yaygınlaşması, kullanıcıların bilgiye erişimini kolaylaştırmakla birlikte siber güvenlik açıklarını da beraberinde getirmiştir. Özellikle kimlik avı gibi sosyal mühendislik tabanlı saldırıların QR kodlar aracılığıyla gerçekleştirilebilmesi, bu teknolojinin güvenliğine dair farkındalığın ne derece kritik olduğunu ortaya koymaktadır. Mevcut literatür incelendiğinde, QR kodların potansiyel bir tehdit aracı olarak ele alınmasına yönelik çalışmaların sınırlı olduğu; özellikle üniversite öğrencileri gibi teknolojiye hakim genç yetişkinler arasında bu farkındalığı ölçmeyi hedefleyen ampirik araştırmaların eksik olduğu görülmektedir. Bu bağlamda, söz konusu boşluğu doldurmayı amaçlayan bu çalışma Karadeniz Teknik Üniversitesi kampüsüne yerleştirilen QR kodlu afişler aracılığıyla kullanıcıların tarama motivasyonları ve güvenlik farkındalıkları analiz edilmiştir. Kampüs içine resimli ve resimsiz QR kodlu afişler asılarak, kullanıcıların bu kodları okutması sağlanmış ve ardından bir ankete yönlendirilmişlerdir. Ankete verdikleri cevaplar üzerinden bir farkındalık analizi yapılması hedeflenmiştir. Ayrıca, afiş tasarımında kullanılan görsel unsurların kullanıcı davranışları üzerindeki etkisinin ölçülmesi bakımından literatüre özgün bir katkı sunmaktadır. Bununla birlikte, çalışmanın yalnızca tek bir üniversite ile sınırlı olması ve yalnızca nicel yöntem kullanılarak gerçekleştirilmiş olması, genellenebilirlik açısından önemli bir sınırlılıktır. Ancak bu sınırlılık, çalışmanın bağlamsal derinliğini hedeflemesi ve saha temelli ampirik veri üretmesi nedeniyle, alan literatürüne kıymetli katkılar sağlamaktadır. Çalışmanın ikinci bölümünde, QR kodlarının farklı kullanım alanları, bu kodlar üzerinden gerçekleştirilebilecek saldırılar, özellikle kimlik avı saldırıları ve bu saldırıların önemi

üzerinde durulmuştur. Üçüncü bölümde ise, yapılan çalışmanın araştırma yöntemi, analiz ve bulgularına yer verilmiş, ardından sonuçlar ve değerlendirme ile çalışma tamamlanmıştır.

1. LİTERATÜR

QR kod sistemi, geleneksel barkodlara kıyasla sunduğu avantajlarla fiziksel ve dijital alanları reklam ve tanıtım için etkili birer vitrine dönüştürmektedir. Sosyal hayatın her alanında erişimi kolaylaştırmasıyla kullanımı artan bu teknoloji hemen her yerde QR kodla karşılaşılabilme ihtimalini arttırmaktadır (Örücü, 2013). Televizyon reklamları, yazılı basın, süreli yayınlar ve kartvizitler gibi birçok alanda yer alarak hayatı büyük ölçüde kolaylaştırmaktadır (Amoah & Hayfron-Acquah, 2022).

QR kodlar, bilgileri siyah ve beyaz karelerden oluşan bir matris şeklinde kodlayan sistemle çalışır. Dijital bir cihaz, QR kodu taradığında, cihazın kamerası bu deseni algılar ve QR kod okuyucu uygulaması, desende saklanan bilgileri (Hoy, 2011; Ismail vd., 2021; Alde & Humbe, 2024). Kodlanan bu bilgiler, bir web sayfasını açma, bir metin gösterme veya bir telefona iletişim bilgileri kaydetme gibi çeşitli işlemleri başlatabilir (Hoy, 2011; Thamilselvan & Mohanasundaram, 2019).

QR kodlar, dijitalleşen dünyada farklı alanlarda yaratıcı kullanımlarıyla dikkat çekmektedir. Örneğin, vCard (Elektronik Kartvizit) teknolojisi sayesinde kartvizitler dijitalleşmiş, Pet Shop Boys ve Kylie Minogue gibi sanatçılar QR kodları müzik çalışmalarında tanıtım aracı olarak kullanmıştır. Ayrıca, 2008'de Avustralyalı sanatçı Simone O'Callaghan, QR kod temelli baskı sanatıyla izleyicilere online bir deneyim sunarken, Duncan Robertson QR kodlarla BBC haberlerine kolay erişim sağlamıştır. Bu sayede QR kodlar, sanat ve teknolojinin kesişiminde yenilikçi uygulamaların önünü açmıştır (Arslan, 2011). Ayrıca, harita uygulamalarıyla entegrasyonu sayesinde mağazaların konumlarını kolayca göstererek, özellikle yeni açılan mağazalar için önemli bir avantaj sağlamıştır (Bozkurt & Ergen, 2012; Sanal & Öztürkoglu, 2017).

QR kodların kullanımının artması güvenlik risklerini de beraberinde getirmiştir. QR kodlar ile kullanıcılar manipüle edilmek üzere tasarlanmış kötü amaçlı web sitelerine yönlendirilebilir. Saldırganlar, etiketlere kötü amaçlı QR kodları basabilir ve bunları güvenilir olan QR kodların üzerine yerleştirebilir. Bu da kullanıcıların farkında olmadan zararlı web sitelerine yönlendirilmesine neden olmaktadır (Krombholz vd., 2014; Goel vd., 2017). Bir QR kod okuyucusu kodlanmış verilere doğrudan erişebildiği için hassas bilgileri kolayca ifşa edebilir. Bu erişim, ek güvenlik önlemleri olmadan QR kodlarının gizli bilgi aktarımı için uygun olmadığını göstermektedir (Zhu, 2014; Alde & Humbe, 2024). Bir QR kodunun taranması, kötü amaçlı kodun çalışmasına neden olarak kullanıcının cihazını riske atabilir ve hassas bilgilerin çalınmasına yol açabilir (Bani-Hani vd., 2014). Bu tür güvenlik açıkları ile QR kod, kimlik avı saldırıları gibi kötü amaçlı faaliyetler için de etkili bir saldırı yöntemi olabileceğini kanıtlamıştır (Krombholz vd., 2015).

Kimlik avı saldırıları, kişileri kullanıcı adları, parolalar, kredi kartı bilgileri ve diğer kişisel veriler gibi hassas bilgileri ifşa ederek kandırmayı içeren bir siber saldırı biçimidir (Mahalakshmi vd., 2018). Bu saldırılar, sahte e-postalar ve web siteleri yoluyla güvenilir

kurumları taklit ederek kurbanları hedef alır ve belirli bir bağlantıya yönlendirerek bilgi toplar (Piper, 2007). İlk kez 1996’da ortaya çıkan kimlik avı, günümüzde en ciddi çevrimiçi tehditlerden biri haline gelmiştir (Varshney vd, 2016). İnternet kullanıcılarının sosyal medya veya e-posta yoluyla iletilen bağlantıların doğruluğunu kontrol etmesi doğrudan veri girişi talep eden web sitelerine karşı bilinçli ve dikkatli davranmaları büyük önem taşımaktadır (Chen vd., 2014).

Kimlik avı saldırıları yalnızca e-posta, truva atı veya virüslerle sınırlı olmayıp, QR kodlar gibi araçlarla da gerçekleştirilebilmektedir. Kullanıcıların bu tür saldırılar konusunda farkındalığı ve alınan önlemler artsa da saldırganlar sürekli olarak yeni dolandırıcılık yöntemleri geliştirmektedir. Dolandırıcılar, halka açık ve yoğun trafiğe sahip alanlarda QR kodları kullanarak, QRishing (QR Kodlu Kimlik Avı) adı verilen bir kimlik avı türüyle kullanıcıları hedef alabilmektedir. Bu yöntem, sosyal mühendislik teknikleriyle QR kod taramaları üzerinden kişisel bilgileri ele geçirmeyi amaçlamaktadır (Ahuja, 2014). QR kodlar dağıtılması ve üretilmesinin kolaylığı sayesinde reklam panolarından ürün ve hizmet alıcılarına kadar bilgilerin dağıtılmasında kolaylık sağlaması saldırganlar tarafından kullanıcıların hayati bilgilerini elde etmek için bir saldırı vektörü haline gelmiştir (Kharraz vd, 2014; Krombholz vd, 2014).

Her ne kadar QR kodlar üzerinden gerçekleştirilebilecek çeşitli saldırı türleri bulunsada, literatürdeki çalışmalar kullanıcıların bu teknolojiyi potansiyel bir saldırı aracı olarak algılamadığını ortaya koymaktadır. Bu durumu inceleyen Vidas ve arkadaşları (2012), gerçekleştirdikleri araştırmada iki aşamalı bir deneysel tasarım benimsemiştir. İlk aşamada yürütülen “QRishing” deneyinde, Carnegie Mellon Üniversitesi kampüsü ile Pittsburgh şehrindeki çeşitli kamusal alanlara dört farklı ilan yerleştirilmiş ve bu ilanlar dört hafta boyunca sergilenmiştir. QR kodları tarayan kullanıcılar doğrudan çevrimiçi bir ankete yönlendirilmiştir. İkinci aşama olan “Gözetim” deneyinde ise, QR kodlarını taradıktan sonra anketi tamamlamayan bireylerin sayısının belirlenebilmesi amacıyla kullanıcı davranışları kamera ile izlenmiştir. Çalışma bulgularına göre, toplamda 225 kişi ilgili web sayfasını ziyaret etmiş, bunların 122’si anketi doldurmuştur. QRishing deneyinden elde edilen veriler, kullanıcıların QR kodları tarama eylemlerinde en belirgin motivasyonun merak olduğunu göstermiştir. Gözetim deneyinin sonuçları ise QR kodu tarayan katılımcıların %85’inin bağlantıyı ziyaret ettiğini ortaya koyarak, kullanıcıların potansiyel tehditlere karşı farkındalık düzeyinin düşük olduğunu göstermiştir.

Kapsalis (2013) tarafından Viyana, Helsinki, Atina ve Paris şehirlerinde gerçekleştirilen çalışmada, QR kodların bireylerde oluşturduğu güvenlik bilinci düzeyini ölçmek amacıyla çeşitli konumlara üç farklı QR kod yerleştirilmiştir. Çalışma kapsamında toplam 273 kişi bu kodları taramış, ancak yalnızca 83 katılımcı anketi tamamlamıştır. Anket verilerinin analizi sonucunda, kullanıcıların QR kod tarama eylemlerindeki temel motivasyonun merak duygusu olduğu belirlenmiş; ayrıca katılımcıların büyük bir bölümünün QR kodların potansiyel güvenlik tehditleri konusunda yeterli bilgiye sahip olmadığı tespit edilmiştir.

Yin vd. (2013) akıllı telefonlarla QR kod kullanımının güvenlik riskleri üzerine yaptıkları çalışmada, kullanıcıların kötü niyetli web sayfasına yönlendirildiği aşamada gelen uyarı mesajına verdikleri tepkiler incelenmiştir. Çevrimiçi anket kullanılarak yapılan çalışmaya toplamda 182 yüksek lisans öğrencisi katılmıştır. Çalışmanın sonucunda cinsiyet, coğrafi konum ve daha önce QR kod tarama deneyiminin uyarı mesajını dikkate alınmaması üzerinde bir etkisi olmadığı sonucuna varılmıştır. Ayrıca, bilişim teknolojileri alanında tecrübe sahibi olan katılımcıların uyarı mesajını görmezden gelme olasılıklarının daha yüksek olduğu sonucuna varılmıştır.

Türkiye’de ise Başaran & Göksel (2016) tarafından gerçekleştirilen çalışmada Ankara, İstanbul ve Kıbrıs’taki çeşitli yerlere QR kod afişleri asılmıştır. Zararsız olan bu QR kodlar okutulduğunda kullanıcılara oltalandıklarına dair bilgi mesajı gösterilmiştir. 3 ay boyunca bu trafik izlenmiş ve QR kodlar toplam 9027 kullanıcı tarafından okutulmuştur.

QR kodlar ile hem sosyal mühendislik saldırıları hem de otomatik sistemlere saldırılar yapılabilir. SQL ve komut enjeksiyonu, bilgisayar korsanları tarafından otomatik sistemlere kolaylıkla enjekte edilebilir. Örneğin, bir QR kod çözme yazılımının bir veritabanına bağlı olduğunu ve arka planda bir sorgu yürütmek için QR kod bilgilerinden yararlandığını varsayalım. Böyle bir senaryoda, QR kodun SQL enjeksiyonuna sebep olacak “1’ OR ‘1’=1” gibi bir ifade içermesi durumunda (tırnak işaretleri hariç), sistem, QR kodunun güvenilir bir kaynaktan gelip gelmediğini doğrulamadan sorguyu çalıştırabilir. Bu durum, yalnızca yetkili kullanıcılar için tasarlanmış bilgilere, kötü niyetli kişilerin erişmesine yol açabilir. QR kodlarının şu anda veritabanı sorgulamaları yürütmek amacıyla yaygın olarak kullanılmadığı görülse de gelecekte bu tür sistemlere yönelik saldırılarda kullanılma potansiyeli mevcuttur. Nitekim, Google gibi büyük platformlar, kullanıcı hesaplarına girişte QR kodlarının kullanılmasına yönelik denemeler gerçekleştirildiği bilinmektedir (Sharma, 2012).

Komut Enjeksiyonu yöntemiyle, saldırgan bir HTML kodu enjekte ederek sayfa içeriğini değiştirebilir. Kurban kullanıcı tarattığı QR kod aracılığı ile söz konusu sayfayı ziyaret ettiğinde, web tarayıcısının zararlı kodu yorumlaması sonucu cihazında (genellikle akıllı telefon ya da tablet) kötü amaçlı komutların çalıştırılmasına sebep olabilmektedir (Ahuja, 2014). Başka bir deyişle, QR koddan gelen verilerin komut satırı parametresi olarak kullanıldığı bir senaryoda, saldırgan QR kodu manipüle ederek sistemde rastgele komutlar çalıştırabilir. Böyle bir saldırı sonucunda rootkit (kök yazılım), casus yazılım (spyware), Servis Engelleme (DoS) saldırıları başlatılabilir veya uzaktaki bir bilgisayara bağlanarak sistem kaynaklarına erişim sağlanabilir (Sharma, 2012).

Sosyal mühendislik tabanlı saldırılarda QR kodların kullanım şekillerine bakıldığında, saldırganlar hedef aldıkları kitleyi özel tekliflerle ya da belirli ürünler hakkında bilgi vermek amacıyla QR kodun taratılmasını amaçlamaktadırlar. Saldırganlar QR kodları manipüle ederek kurbanı farkına varmadan sahte bir sayfaya yönlendirir. Bu tür bir senaryoda, saldırgan QR koda bir URL adresi kodlayarak, kullanıcının QR kodu taramasıyla kötü amaçlı yazılımın otomatik olarak kurbanın cihazına indirileceği bir sayfaya yönlendirme

yapabilir. Bu yöntemle virüs, casus yazılım, truva atı, solucan ya da kullanıcı ve cihazı için ciddi zararlara yol açabilecek zararlı yazılımların yayılması sağlanabilir. Bunun yanı sıra sosyal medya üzerinden kullanıcılara ulaşan sahte banka reklamları, çekilişe katılma hakkı veya ödül kazanma gibi vaatlerle kullanıcıları kandırarak sahte internet sitelerine yönlendirebilmektedir. Kullanıcılar, linke tıklayıp giriş bilgilerini ve banka tarafından gönderilen doğrulama şifresini bu sahte siteye girdiğinde, dolandırıcılar bu bilgileri ele geçirerek bankada kurban adına işlem yapabilmektedir. Bu yöntemle saldırganlar, QR kodunu kullanarak ATM'den kart olmadan para çekebilir, hesapları boşaltabilir veya kullanıcı adına kredi çekebilir. Türkiye'de bu tür bir dolandırıcılık girişimi, siber suçlarla mücadele birimleri tarafından engellenmiştir (Bilir & Özkoç, 2020). Benzer şekilde, Çin Halk Cumhuriyeti Merkez Bankası, QR kod tabanlı ödemelerin kara para aklama ve dolandırıcılık için kullanıldığı gerekçesiyle bu tür işlemleri yasaklama kararı almıştır (Webtekno, 2017).

QR kod saldırılarına karşı alınacak önlemler arasında, kullanıcılar sosyal mühendislik saldırılarına karşı dikkatli olmalı ve kaynağı bilinmeyen QR kodlarını taramamalıdır (Krombholz vd., 2014). QR kodların içerdiği verilerin güvenli olarak saklanabilmesi için AES (Advanced Encryption Standard) gibi kriptografik yöntemlerden yararlanılabilir. Bu sayede, yalnızca doğru anahtara sahip yetkili kullanıcılar bilgilere erişebilecektir (Goel vd., 2017; Focardi vd., 2019). Gerçek zamanlı kimlik avı ve kötü amaçlı yazılım içeren URL'leri tespit edebilen QR kod okuyucuların yanında, makine öğrenim modellerinin kullanımı kötü amaçlı bağlantıları belirlemede etkili bir yöntem olarak ortaya çıkmaktadır (Wahsheh & Al-Zahrani, 2021). Ayrıca QR koda dijital bir filigran yerleştirerek güvenliği artırabilir. Yuwei & Su (2020), QR kod güvenliğini artırmak için yaptıkları çalışmada dijital filigran teknolojisi kullanılmıştır. Bu yöntem, QR kodun sahte olup olmadığını doğrulamayı ve içeriğin değiştirilmesini önlemeyi amaçlar. Yöntemde, QR kod 8x8 bloklara ayrılır ve her blok üzerinde 2D-DCT (Two-Dimensional Discrete Cosine Transform) uygulanır. Bu dönüşüm, filigranın görünmezliğini artırırken kodun dayanıklılığını korur. Daha sonra, SVD (Singular Value Decomposition) yöntemiyle filigran bilgisi, her bloğun orta kısmına gömülür. Bu yöntem, filigranın saldırılara karşı dayanıklılığını artırır ve yüksek kaliteli geri alma sağlar.

Mevcut literatür incelendiğinde, QR kodlarının güvenliği konusunda kullanıcı farkındalığına dair yapılan ampirik çalışmaların sayısı sınırlıdır. Özellikle kampüs ortamında, üniversite öğrencilerinin QR kodlar ile ilgili farkındalık düzeyini ölçmeye yönelik çalışmalar daha azdır. Bu çalışma hem bu boşluğu doldurmayı hem de Karadeniz Teknik Üniversitesi kampüsünde üniversite öğrencilerinin QR kod kullanımındaki güvenlik farkındalığını saha araştırmasıyla ölçmeyi amaçlamaktadır.

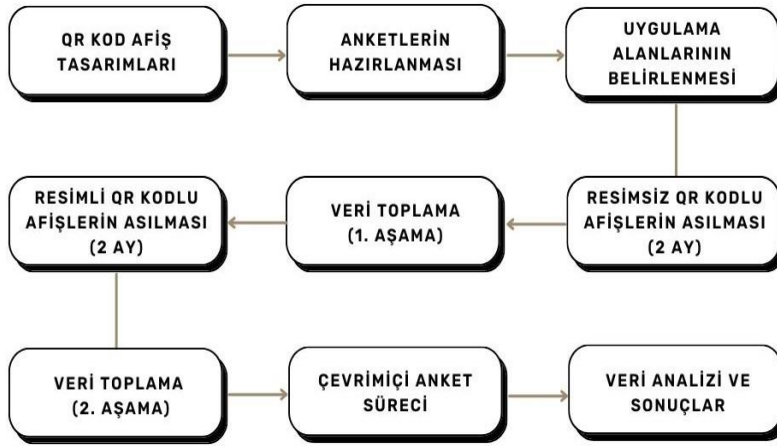
2. YÖNTEM

Çalışmada, kullanıcıların QR kod farkındalık düzeyleri ve QR kodları tarama motivasyonları araştırılmıştır. Bu doğrultuda, iki farklı türde QR kod afişi tasarlanmıştır. Resimsiz QR kodlu afişler, basit ve renksiz bir QR kod ile QR kodun içeriğine dair sade bir

metin içermektedir. Resimli QR kodlu afişler ise dikkat çekici, renkli temalarla zenginleştirilmiş ve kullanıcı ilgisini artırmayı hedefleyen çeşitli görsellerle donatılmıştır. Her iki afiş türüne ilişkin örnekler, Ek bölümünde bulunan Şekil 12, Şekil 13, Şekil 14 ve Şekil 15'te gösterilmiştir. Çalışmada nicel araştırma yöntemi kullanılmış olup, veri toplama aracı olarak çevrimiçi anket kullanılmıştır. Kullanıcıların QR kodları taradığında yönlendirildiği çevrimiçi anketin genel görünümü Ek'te yer alan Şekil 16'da gösterilmiştir. Bu ankette Bilir & Özkoç (2020)'un çalışmasında kullanılan ölçek temel alınmış ve ek sorularla zenginleştirilmiştir. Kullanıcılar anket sayfasına yönlendirildiğinde bir uyarı mesajı ile karşılaşmışlardır.

Çalışmada, teknoloji farkındalığı yüksek bireyleri hedeflemek amacıyla, araştırmanın veri toplama süreci yalnızca Karadeniz Teknik Üniversitesi kampüsünde gerçekleştirilmiştir. Katılımcıların büyük çoğunluğunu benzer demografik ve akademik özelliklere sahip bireyler oluşturmaktadır. Bu durum, elde edilen bulguların farklı sosyo-kültürel gruplara genellenebilirliğini sınırlamaktadır. Ayrıca, çalışmada yalnızca nicel veri toplama yöntemi kullanılmış, nitel gözlem, derinlemesine görüşme veya odak grup gibi nitel teknikler uygulanmamıştır. Bu da katılımcıların QR kod tarama davranışlarının altında yatan bilişsel, duygusal ve sosyal faktörlerin derinlemesine analizini sınırlamaktadır. Gelecek çalışmalarda, nitel verilerin de dahil edildiği karma yöntem tasarımları tercih edilerek daha kapsamlı bir değerlendirme yapılması önerilmektedir. Özellikle merak, güven, risk algısı, alışkanlık ve sosyal etkileşim gibi değişkenlerin kullanıcı davranışına etkisi, nitel verilerle desteklenerek daha açıklayıcı biçimde ortaya koyulabilir. Veri toplama alanı olarak, afişlerin tasarımlarının içeriği de göz önünde bulundurularak; kampüs içindeki duraklar, kafeler, yemekhane, kantin ve fakültelerin duyuru panoları gibi öğrenci yoğunluğunun yüksek olduğu yerler seçilmiş, her iki afiş türü eşit miktarda olacak şekilde kampüs genelinde belirtilen alanlara yerleştirilerek kullanıcıların QR kod tarama davranışları gözlemlenmiştir. Asılan afişlerin örnekleri Ek'teki Şekil 17 ve Şekil 18'de gösterilmiştir. Toplanan veriler, yüzde dağılımlarının yanı sıra, kategorik değişkenler arasındaki ilişkiyi incelemek amacıyla Pearson ki-kare testi ile analiz edilmiştir.

Afişlerin asılı kalma süresi, çalışmanın gerçekçi ve güvenilir sonuçlar ortaya koyabilmesi amacıyla 2 ay olarak belirlenmiştir. Bu süre, hava koşulları, öğrencilerin yoğunluk durumu gibi çeşitli faktörlerin etkisini dengelemek için tercih edilmiştir. Ayrıca, önceki araştırmalarda benzer saha çalışmalarında ortalama 2 aylık sürelerin güvenilir veri toplama açısından yeterli olduğu görülmüştür. Araştırmanın ilk aşamasında, resimsiz QR kodlu afişler belirtilen noktalara yerleştirilmiş ve 2 ay boyunca kullanıcı davranışları izlenmiştir. İkinci aşamada, aynı noktalara eşit miktarda resimli QR kodlu afişler asılmış ve bu afişler 2 ay boyunca yerinde bırakılarak veri toplama süreci devam etmiştir.



Şekil 1: Metodolojik Akış Diyagramı

Çalışmanın metodolojisini sistematik bir şekilde gösterebilmek amacıyla, süreç bir akış diyagramı ile görselleştirilmiştir. Şekil 1’de, çalışmanın aşamaları adım adım sunulmuştur. Bu diyagram, araştırmanın veri toplama sürecini, afişlerin yerleştirilmesini ve anket sürecini özetlemektedir.

3. ANALİZ VE BULGULAR

Bu çalışmanın amacı, QR kod farkındalığını ölçmek ve QR kod tabanlı kimlik avı saldırılarının kullanıcılar üzerindeki etkisini incelemektir. Bu doğrultuda Karadeniz Teknik Üniversitesi kampüs içerisine resimli ve resimsiz QR kodlu afişler yerleştirilmiş ve kullanıcılar çevrimiçi bir ankete yönlendirilmiştir. Anket, katılımcıların QR kodları tarama motivasyonlarını, demografik bilgilerini ve QR kod tabanlı kimlik avı saldırıları hakkında ne kadar bilgi sahibi olduklarını ölçmeyi hedeflemiştir. Çalışmanın ikinci bölümünde QR kodların kullanım alanları, bu kodlarla yapılabilecek kimlik avı saldırıları ve bu saldırıların kullanıcılar üzerindeki potansiyel tehditleri ele alınmıştır. Bu bölümde ise elde edilen veriler analiz edilerek, QR kodların kullanıcılar tarafından nasıl algılandığı ve hangi faktörlerin QR kod tabanlı kimlik avı saldırılarına karşı duyarlılığı etkilediği üzerine bulgular sunulacaktır.

Çalışmada elde edilen verilere göre, toplamda 535 QR kod okunması gerçekleşmiştir. Bu okunmaların 450’si (%84) resimli QR kodlu afişlerden, 85’i (%16) ise resimsiz QR kodlu afişlerden oluşmaktadır. Elde edilen bu sonuçlar, resimli QR kodlu afişlerin kullanıcılar tarafından daha fazla ilgi çektiğini göstermektedir. Kullanıcıların, görsel olarak daha cazip ve dikkat çekici tasarımlarla oluşturulmuş QR kodları daha fazla tarama eğiliminde olduğu görülmüştür.

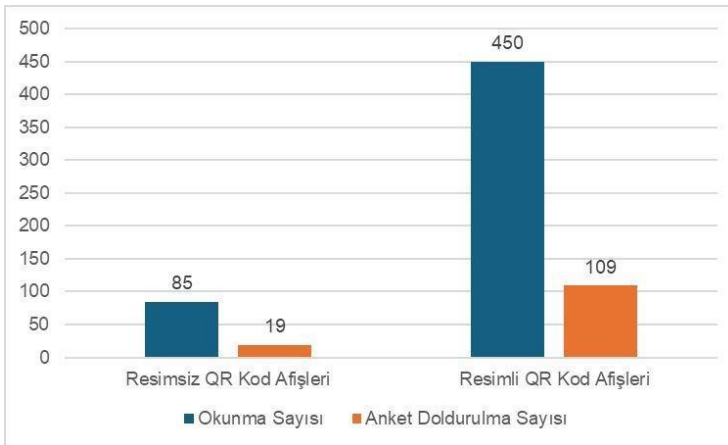
Literatürde, renk ve grafikler gibi görsel öğelerin bir posterdeki genel izlenimi önemli ölçüde artırdığı belirtilmektedir. Bu tür öğelerin etkili kullanımı, posterleri estetik açıdan daha hoş ve ilgi çekici hale getirebilmektedir (Ellerbee, 2009; Wen vd., 2022). Çalışmamızın bulguları da bu görüşü desteklemekte olup, QR kodların görsel açıdan zenginleştirilmesinin kullanıcıların tarama eğilimlerini doğrudan etkileyebileceğini ortaya koymaktadır.

Katılımcıların, görsel olarak daha dikkat çekici tasarımlarla oluşturulmuş QR kodları daha fazla tarama eğiliminde olduğu gözlemlenmiş olsa da bu etkileşimin davranış düzeyince bir farklılık yaratıp yaratmadığını belirlemek amacıyla Pearson ki-kare (χ^2) testi uygulanmıştır. Resimsiz QR kodlu afişlerin 85 kez tarandığı ve bunlardan 19'unun anket doldurduğu; resimli QR kodlu afişlerin ise 450 kez tarandığı ve 109'unun anket doldurduğu belirlenmiştir. Elde edilen sonuçlara göre, iki afiş türü arasında doldurma davranışı açısından istatistiksel olarak anlamlı bir fark bulunmamıştır, $\chi^2(1, N=535) = 0.054$, $p = 0.817$. Bu bulgu, görsel zenginliğe sahip olan QR kodlu afişlerin kullanıcıların ilk etkileşimini artırmış olabileceğini, ancak bu görselliğin kullanıcıları anket doldurma gibi sonraki davranışlara yönlendirmede belirleyici bir faktör olmadığını göstermektedir.

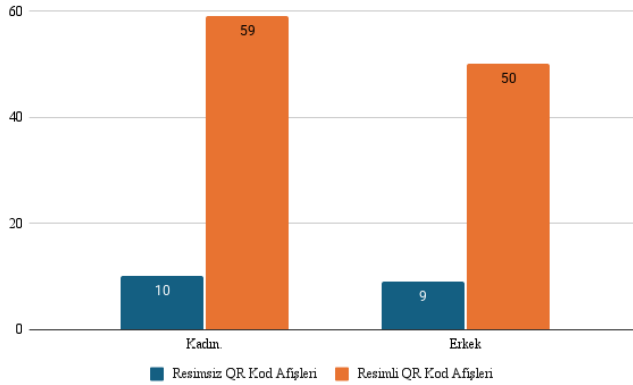
Resimsiz QR kodlu afişleri okutan 85 kişiden 19'u (%22.35) anketi doldururken, resimli QR kodlu afişleri okutan 450 kişiden 109'u (%24.22) anketi doldurmuştur. Anket doldurma oranları benzer olsa da renkli QR kodlar daha fazla kişi tarafından tarandığı için toplamda daha fazla anket yanıtı alınmıştır. Bu da resimli QR kodların daha fazla tarama eğiliminde olduğunu desteklemektedir. İlgili dağılım ve oranlar, Tablo 1 ve Şekil 2'de ayrıntılı bir şekilde sunulmuştur.

Tablo 1: Okunma ve Anket Doldurma Sayısı

Afiş Türü	Okunma Sayısı	Anket Doldurma Sayısı	Anket Doldurma Oranı
Resimsiz QR Kod Afişi	85	19	%22,35
Resimli QR Kod Afişi	450	109	%24,22
Toplam	535	128	%23,93

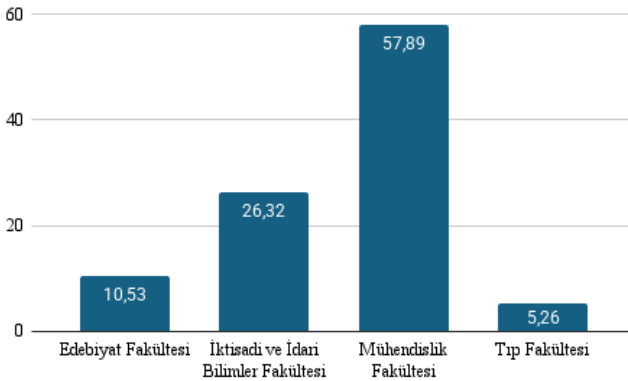


Şekil 2: Okunma ve Anket Doldurma Sayısı

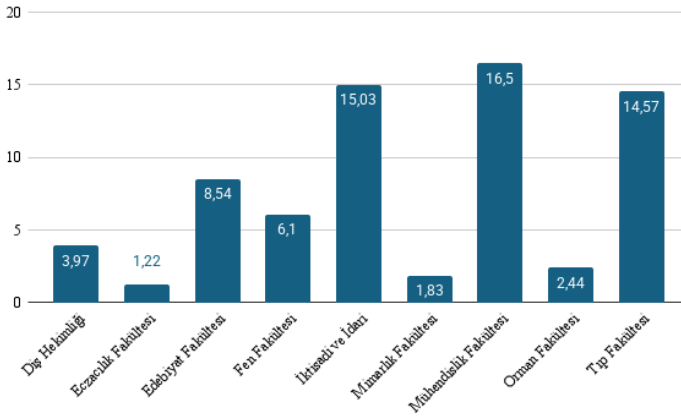


Şekil 3. Anket Dolduran Katılımcıların Cinsiyet Dağılımı

Şekil 3'te verilen Anket Dolduran Katılımcıların Cinsiyet Dağılımı grafiği incelendiğinde tüm afişler dikkate alındığında, ankete katılan 128 kişinin %53,9'u (69 kişi) kadın, %46,1'i (59 kişi) erkektir. Resimsiz QR kodlu afişleri tarayıp ankete katılan 19 kişinin %52,6'sı (10 kişi) kadın, %47,4'ü (9 kişi) erkektir. Resimli QR kodlu afişleri tarayıp anket dolduran 109 kişinin ise %54,1'i (59 kişi) kadın, %45,9'u (50 kişi) erkektir. Sonuçlar incelendiğinde, resimli QR kodlu afişlerin, resimsiz olanlara kıyasla yaklaşık 5,3 kat daha fazla tarandığı görülmektedir. Katılımcılar arasında kadınlar, erkeklere kıyasla daha yüksek sayıda anket katılımı sağlamıştır. Bu bulgular, her iki durumda da kadınların daha yüksek bir QR kod tarama oranına sahip olduğunu göstermektedir. Literatürde, kadınların kimlik avı saldırılarına karşı erkeklerden daha savunmasız olduğuna dair bulgular yer almaktadır (Sheng vd., 2010; Liu vd., 2020). Bunun yanı sıra, QR kod tabanlı kimlik avı saldırılarında da benzer bir cinsiyet farklılığının mevcut olduğu ve erkekler ile kadınların siber güvenlik bilgisi ve kimlik avı girişimlerine verdikleri tepkiler açısından anlamlı farklılıklar gösterdiği ifade edilmektedir (Pratama vd., 2023). Çalışmamızda kadın katılımcıların QR kodları tarama oranının erkeklere kıyasla daha yüksek olması, bu farklılığın QR kod farkındalığı bağlamında da değerlendirilebileceğini göstermektedir.



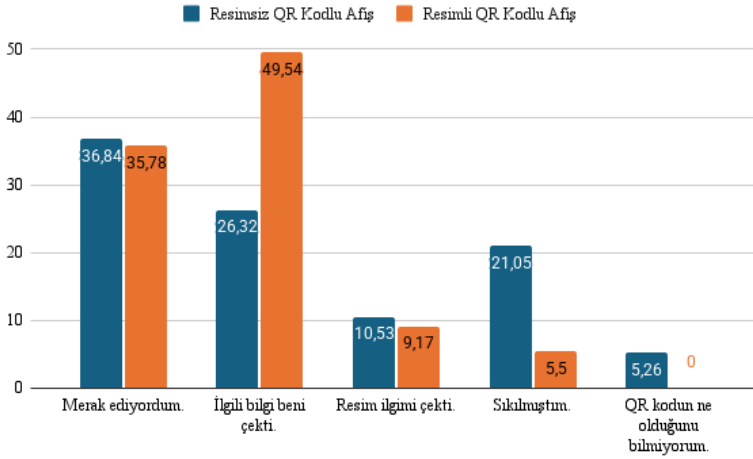
Şekil 4: Anket Dolduran Katılımcıların Fakültele Göre Dağılımı (Resimsiz QR Kodlu Afişler)



Şekil 5: Anket Dolduran Katılımcıların Fakülteye Göre Dağılımı (Resimli QR Kodlu Afişler)

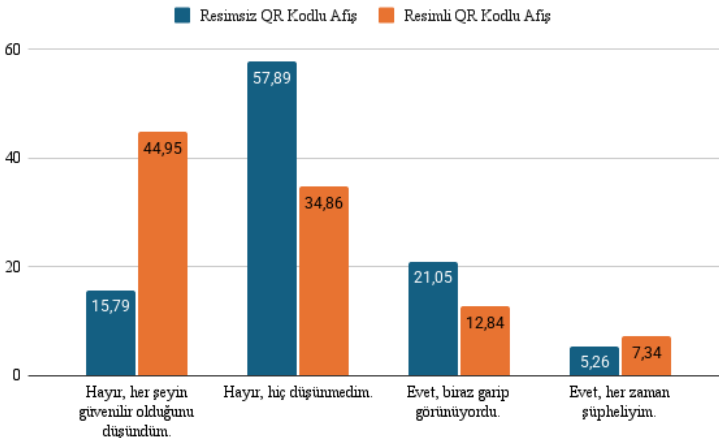
Fakülteye Göre Katılımcı Dağılımı incelendiğinde (Şekil 4 ve Şekil 5), resimsiz QR kodlu afişlerin kullanımının en yüksek olduğu fakülte %57,89 (11 kişi) ile Mühendislik Fakültesi olmuştur. Onu %26,32 (5 kişi) ile İktisadi ve İdari Bilimler Fakültesi takip etmektedir. Diğer fakültelerde resimsiz QR kodlu afişlerin tarama oranı oldukça düşüktür. Resimli QR kodlu afişlerde ise en yüksek ankete katılım oranı %16,50 (25 kişi) ile Mühendislik Fakültesine aittir. Bunu %15,03 (23 kişi) ile İktisadi ve İdari Bilimler Fakültesi, %14,57 (22 kişi) ile Tıp Fakültesi takip etmektedir. Bu sonuçlar, resimli QR kodlu afişlerin tüm fakültelerde daha yüksek oranda tarandığını göstermektedir.

Katılımcılardan yaş bilgisi alınmamış olmakla birlikte, araştırmanın gerçekleştirildiği üniversite ortamı gereği katılımcıların büyük çoğunluğunun teknoloji okuryazarlığı yüksek 18-25 yaş arasındaki genç yetişkinlerden oluştuğu varsayılmaktadır. Literatürde, 18-25 yaş aralığındaki bireylerin daha yaşlı gruplara kıyasla kimlik avı saldırılarına karşı daha savunmasız olduğu belirtilmektedir (Sheng vd., 2010; Li vd., 2020). Bu eğilim, QR kod tabanlı kimlik avı saldırılarında da gözlemlenmekte olup, genç nesillerin daha düşük farkındalık düzeyine sahip olmalarına rağmen dijital güvenliklerine daha fazla güvendikleri ifade edilmektedir (Sheng vd., 2010; Pratama vd., 2023). Çalışmamızda da benzer bir durum gözlemlenmiş olup, genç katılımcıların QR kodları tarama oranlarının yüksek olmasına rağmen, güvenlik farkındalıklarının beklenenden düşük olduğu görülmüştür.



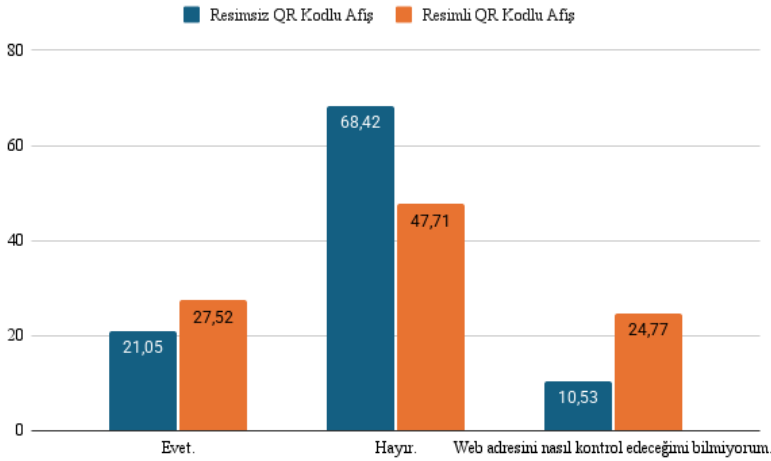
Şekil 6: QR Kod Tarama Motivasyonları Durumu

QR Kod Tarama Motivasyonları incelendiğinde (Şekil 6), resimsiz QR kodlu afişlerde ‘Merak ediyordum’ (%36,84) (7 kişi), resimli QR kodlu afişlerde ise ‘İlgili bilgi beni çekti’ (%49,54) (54 kişi) en sık belirtilen nedenlerdir. Ayrıca, resimsiz QR kodlu afişlerde ‘Sıkılmıştım’ yanıtı daha yüksek oranda görülmüş (%21,05) (4 kişi), bu oran resimli QR kodlu afişlerde %5,5 (6 kişi) oranı ile belirgin şekilde düşük kalmıştır. Bulgular, görsel öğelerin bilgiye yönelik ilgiyi artırırken rastlantısal etkileşimi azaltabileceğini göstermiştir. Literatürde, güven ve merak duygusunun kimlik avı duyarlılığının önemli belirleyicileri olduğu belirtilmektedir. Özellikle, bilinen kaynaklardan gelen e-postalar ve merak ya da risk alma davranışını tetikleyen mesajların bireyleri aldatma olasılığının daha yüksek olduğu ifade edilmektedir (Moody vd., 2017). Çalışmamızda da merak unsurunun resimsiz QR kodlu afişlerin taranmasında daha belirleyici olduğu görülmüştür. Bu durum, kimlik avı saldırılarında bireylerin ilgisini çekecek mesajlar ve belirsizlik yaratan öğeler kullanılarak aldatılma riskinin artırılabilceğini göstermektedir.



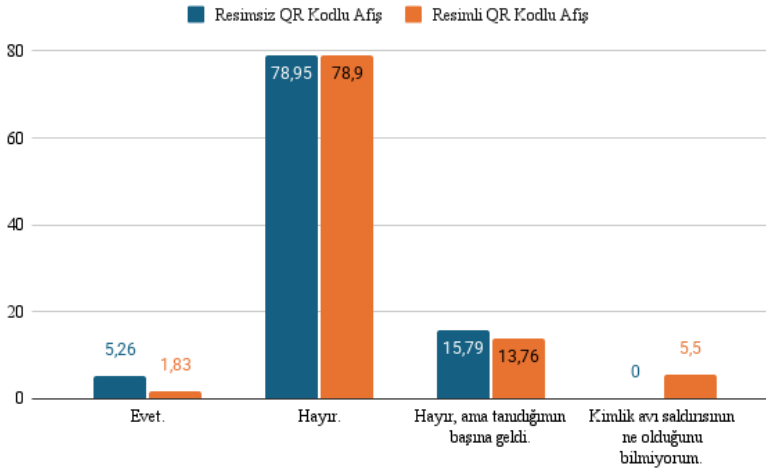
Şekil 7: Şüphe Duyma Durumu

Şüphe Duyma Durumu hakkında sorulan soruya verilen yanıtlar Şekil 7’de gösterilmiştir. Katılımcıların QR kodların güvenilirliği konusundaki algıları incelendiğinde, resimli QR kodlu afişleri tarayanların %44,95’i (49 kişi) ‘Her şeyin güvenilir olduğunu düşündüm’ yanıtını verirken, bu oran resimsiz QR kodlu afişlerde yalnızca %15,79’dur (3 kişi). Resimsiz QR kodlu afişleri tarayanların %57,89’u (11 kişi) güvenlik konusunda hiç düşünmediklerini belirtirken, bu oran resimli QR kodlu afişlerde %34,86 (38 kişi) olarak daha düşük kalmıştır. Ayrıca, ‘Biraz garip görünüyordu’ seçimini yapanların oranı, resimsiz QR kodlu afişlerde (%21,05) (4 kişi), resimli QR kodlu afişlere göre (%12,84) (14 kişi) daha yüksektir. Bu yüzdelik farklılıklar, görsel destekli QR kodların bazı katılımcılar üzerinde daha fazla güven duygusu oluşturabileceğine işaret etmektedir. Ancak Pearson ki-kare testi sonucu, afiş türü ile şüphe duyma düzeyi arasında istatistiksel olarak anlamlı bir fark olmadığını göstermiştir ($\chi^2(3,N=151) = 6.50, p = 0.089$). Bu nedenle, söz konusu farklılıkların tesadüfi olabileceği ve genellenebilir sonuçlar olarak yorumlanmaması gerektiği belirtilmelidir.



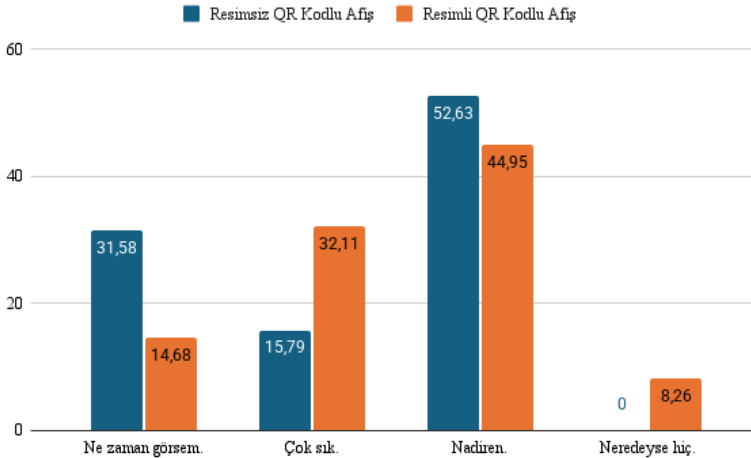
Şekil 8: Web Adresi Kontrolü

Şekil 8’de verilen katılımcıların QR kodlardaki web adresini kontrol etme alışkanlıkları incelendiğinde, resimli QR kodlu afişleri tarayanların %27,52’si (30 kişi) web adresini kontrol ettiğini belirtirken, resimsiz QR kodlu afişlerde bu oran %21,05’te (4 kişi) kalmıştır. Web adresini kontrol etmeyenlerin oranı resimsiz QR kodlu afişlerde %68,42 (13 kişi) iken, resimli QR kodlu afişlerde %47,71 (52 kişi) olmuştur. Bu bulgu, katılımcıların QR kodları tararken web adresine dikkat etme konusunda yeterince bilgi sahibi olmadıklarını göstermektedir.



Şekil 9: Kimlik Avı Saldırısı Durumu

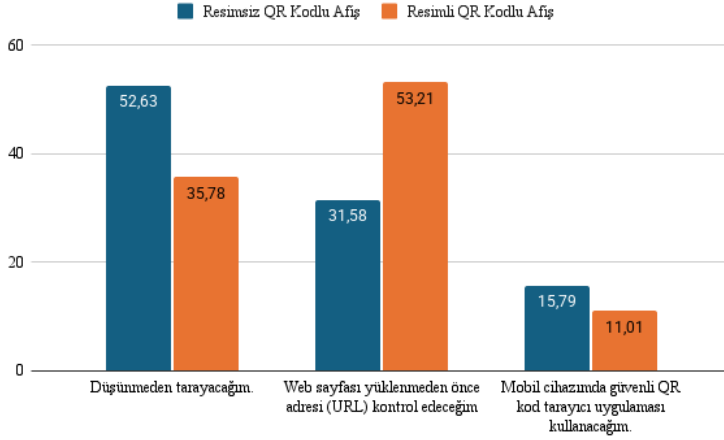
Şekil 9’da sonuçları verilen katılımcıların kimlik avı saldırısına maruz kalma deneyimleri incelendiğinde, hem resimli (%78,90) (15 kişi) hem de resimsiz (%78,95) (86 kişi) QR kodlu afişleri tarayanların büyük çoğunluğu “böyle bir durum yaşamadığını” belirtmiştir. Ancak, ‘Tanıdığının başına geldi’ yanıtı resimsiz QR kodlularda %15,79 (3 kişi), resimli QR kodlularda %13,76 (15 kişi) oranında görülmüştür. ‘Evet, başıma geldi’ yanıtı ise her iki grupta da oldukça düşük olup, resimsiz QR kodlularda %5,26 (1 kişi), resimli QR kodlularda %1,83’tür (2 kişi).



Şekil 10: QR Kodları Tarama Sıklığı

Katılımcıların QR kod tarama sıklıklarına ait veriler Şekil 10’da sunulmuştur. Sonuçlara bakıldığında resimsiz QR kodlu afişleri tarayanların %31,58’i (6 kişi) ‘Ne zaman görsem’ yanıtını verirken, bu oran resimli QR kodlu afişleri tarayanlarda %14,68’dir (16 kişi). Resimli QR kodluları tarayanların %32,11’i (35 kişi) QR kodları ‘Çok sık’ taradığını

belirtirken, bu oran resimsiz QR kodlularda %15,79'dur (3 kişi). 'Nadiren' yanıtı, her iki grupta da en yaygın yanıtlar arasında olup resimsiz QR kodlularda %52,63 (10 kişi), resimli QR kodlularda %44,95'tir (49 kişi). Resimli QR kodlu afişleri tarayanların %8,26'sı (9 kişi) QR kodları 'Neredeyse hiç' taramadığını belirtirken, bu yanıt resimsiz QR kodlarda hiç verilmemiştir. Elde edilen bulgular, katılımcıların genel olarak QR kodları sık kullanmadığını, ancak dikkat çekici ve görsel açıdan zenginleştirilmiş afişlerin bu davranışı olumlu yönde etkileyerek tarama sıklığını artırdığını göstermektedir.



Şekil 11: Katılımcıların Bir Sonraki QR Kod Tarama Davranışı

Katılımcıların gelecekteki QR kod tarama davranışları ile ilgili anket sorusuna verdikleri cevaplar incelendiğinde (Şekil 11), resimsiz QR kodlu afişleri tarayanların %52,63'ü (10 kişi) bir sonraki QR kodu 'Düşünmeden tarayacağımı' belirtirken, bu oran resimli QR kodlu afişleri tarayan kullanıcılarda %35,78 (39 kişi) oranı ile daha düşüktür. Buna karşılık, 'URL kontrol edeceğimi' belirtenlerin oranı resimli QR kodlu afişleri tarayan kullanıcılarda daha yüksek (%53,21) (58 kişi) iken, resimsiz QR kodluları tarayan kullanıcılarda %31,58'dir (6 kişi). Güvenli QR kod tarayıcı uygulaması kullanacağını belirtenlerin oranı ise her iki grupta da düşük seviyede kalmıştır (%15,79 ve %11,01) (3 kişi ve 12 kişi). Bu sonuç, katılımcıların büyük bir kısmının bir sonraki QR kod taramasında daha dikkatli olmayı planladığını, ancak bazı kişilerin hala dikkat etmeden tarama yapmayı tercih edeceklerini göstermektedir.

SONUÇ VE DEĞERLENDİRME

QR kodlar gelişen teknoloji ile hayatımızın her alanında kullanılmaya başlanmış ve bilgi erişimini kolaylaştıran bir araç haline gelmiştir. Hızlı okunabilmesi, geniş bilgi depolama kapasitesi, maliyetinin düşük olması gibi avantajlarıyla hemen hemen her sektörde yoğun bir şekilde kullanılmaktadır. Ancak bu yaygın kullanım beraberinde önemli güvenlik sorunlarını da getirmektedir.

Özellikle bilgi güvenliği bağlamında, QR kodlar kötü niyetli kişiler tarafından zararlı bağlantılar oluşturmak için kullanılabilen ve bu durum kullanıcıları tehlikeye

atmaktadır. SQL Komut Enjeksiyonu, Sosyal mühendislik tabanlı saldırılar ve phishing saldırıları, bu bağlamda en dikkat çekici tehditlerden biridir. Bu tür saldırılar, bireylerin QR konusunda farkındalık düzeyinin düşük olmasından faydalanarak kişisel bilgilerin çalınması gibi kullanıcıları maddi ve manevi olarak etkileyen kayıplara yol açabilir.

Bu çalışmada, teknoloji farkındalığı yüksek bireylerin QR kod zafiyetlerinin yol açabileceği güvenlik sorunlarına karşı farkındalık düzeyleri incelenmiştir. Karadeniz Teknik Üniversitesi kampüsü içerisinde, farklı alanlara resimli ve resimsiz QR kod barındıran afişler yerleştirilmiştir. QR kod afişleri toplamda 535 kişi tarafından taranmış olması, bu afişlerin gerçek bir saldırının parçası olması durumunda 535 kişinin saldırıya maruz kalacağı anlamına gelmektedir. Bu durum, teknolojik farkındalığı yüksek bireylerde dahi QR kod tabanlı saldırılara karşı farkındalık düzeyinin yetersiz olduğunu göstermektedir.

Katılımcıların QR kodları tarama motivasyonunda merak duygusunun ön planda olduğu ve şüphe duysalar bile bu kodları taramaya eğilimli oldukları belirlenmiştir. Ayrıca, QR afiş türünün de bireylerin QR kod okuma davranışını etkilediği, resimli QR kod afişlerinin resimsiz olanlara kıyasla daha fazla tarandığı görülmüştür. Bunun yanı sıra, katılımcıların daha önce kimlik avı saldırısına maruz kalmamış olması, olası QR kod saldırılarına karşı farkındalık düzeylerinin düşük olduğunu desteklemektedir. Bu tür güvenlik açıklarının önüne geçilmesi için en temel adım, bireylerin kaynağı belirsiz QR kodları tarama konusunda daha dikkatli olmalarıdır. Çalışmada kullanılan afişlerde herhangi bir marka ya da güvenilirlik ibaresi bulunmamasına rağmen, kullanıcılar bu kodları tarayarak kaynağı doğrulama davranışını göz ardı etmektedir.

Bununla birlikte, uygulanan istatistiksel analizler sonucunda, gözlemsel olarak ortaya çıkan bazı farkların istatistiksel olarak anlamlı olmadığı görülmüştür. Görsel olarak tasarım ve demografik değişkenler gibi faktörlerin QR kod farkındalığı üzerindeki etkisini test etmek amacıyla gerçekleştirilen Perarson ki-kare analizleri, incelenen değişken çiftleri arasında anlamlı bir ilişki bulunmadığını ortaya koymuştur. Bu durum, QR kodlara yönelik güvenlik farkındalığının yalnızca görsel uyaranlar ya da demografik özellikler değil, bireysel dijital farkındalık ve deneyimle şekillendiğini göstermektedir.

QR kodların güvenli bir şekilde kullanılabilmesi için, taranan kodun URL'sinin kontrol edilmesi, güvenilir QR kod tarama uygulamalarının tercih edilmesi, kamuya açık alanlardaki kodlara karşı dikkatli olunması ve sahte kodlara karşı farkındalığın artırılması gerekmektedir. Ayrıca, cihazların yazılım ve güvenlik güncellemelerinin düzenli olarak yapılması, iki aşamalı doğrulama gibi ek güvenlik yöntemlerinin kullanılması ve QR kodlar üzerinden hassas bilgilerin paylaşılmaması önem arz etmektedir. Bu tür önlemler, QR kod tabanlı tehditlere karşı bireylerin güvenlik düzeyini artırmada etkili yöntemler olacaktır.

Bununla birlikte, çalışmanın bazı kısıtlamaları bulunmaktadır. Öncelikle, araştırma yalnızca Karadeniz Teknik Üniversitesi kampüsüyle sınırlı tutulmuş ve katılımcılar benzer demografik ve akademik özellikler taşıyan bireylerden oluşmuştur. Bu durum, elde edilen bulguların farklı sosyo-kültürel yapılar ve yaş grupları için genellenebilirliğini sınırlamaktadır. Ayrıca, çalışmada yalnızca nicel veri toplanmış; katılımcı davranışlarının

altında yatan psikolojik, duygusal ve sosyal dinamikler incelenmemiştir. Özellikle güven, merak ve risk algısı gibi etkenlerin QR kod tarama davranışı üzerindeki etkileri, nitel yöntemlerle (örneğin yarı yapılandırılmış görüşmeler veya odak grup çalışmaları) desteklenseydi, kullanıcı motivasyonlarına ilişkin daha kapsamlı çıkarımlar yapılabilirdi. Bu doğrultuda, gelecekte gerçekleştirilecek araştırmalarda karma yöntem stratejilerinin benimsenmesi önerilmektedir. Daha geniş bir kullanıcı kitlesi ile, farklı yaş grupları, farklı eğitim seviyeleri, teknoloji bilgisi ve dijital güvenlik farkındalık düzeyleri gibi faktörler göz önünde bulundurularak yürütülecek çalışmalar, QR kod tabanlı kimlik avı farkındalığının demografik değişkenlere göre nasıl farklılaştığını ortaya koyarak alana önemli katkılar sağlayacaktır.

EKLER



Şekil 12: Resimsiz QR Kodlu Afiş



Şekil 13: Resimsiz QR Kodlu Afiş



Şekil 14: Resimli QR Kodlu Afiş



Şekil 15: Resimli QR Kodlu Afiş

DİKKAT! ŞU ANDA OLTALANDINIZ!

Merak etmeyin, bu gerçek bir saldırı değil, yalnızca akademik bir çalışmanın parçasıdır. QR kodları tararken dikkatli olmanız gerektiğini göstermek için tasarlanmış bir farkındalık deneyidir. Bundan sonra, QR kodlarını tararken dikkatli olmayı unutmayın. Ankete katılmak için sonraki sayfaya geçebilirsiniz.

İlerleme durumunu kaydetmek için [Google'da oturum açın](#) Daha fazla bilgi

Bu QR kodu neden taradınız?

☐ Merak ediyordum.

☐ İlgi bilgisi beni çekti.

Şekil 16: Anketin Genel Görünümü



Şekil 17: Resimli QR Kodlu Afiş



Şekil 18: Resimsiz QR Kodlu Afiş

Araştırma ve Yayın Etiği Beyanı

Makalenin yayın süreçlerinde Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Dergisi'nin "Etik Kurallara Uygunluk" başlığı altında belirtilen esaslara uygun olarak hareket edilmiştir. Araştırma için Karadeniz Teknik Üniversitesi Sosyal ve Beşeri Bilimler Etik Kurulu'ndan 11.06.2024 tarih ve E-26014373-050.01.04-520905 numarası ile izin alınmıştır.

Araştırmacıların Katkı Beyanı

Çalışmaya yazarlar eşit oranda katkı sağlamıştır.

Çıkar Çatışması Beyanı

Makalede yazar tarafından beyan edilmiş herhangi bir olası çıkar çatışması bulunmamaktadır.

KAYNAKÇA

- Ahuja, S. (2014). QR Codes and Security Concerns, *International Journal of Computer Science and Information Technologies*, 5(3), 3878-3879.
- Alde, A. B., & Humbe, V. T. (2024). Application of Secure Data Transmission by Integrating QR Code with Visual Cryptography, *Lecture Notes in Networks and Systems*, 1022, 125-133.
- Amoah, G. A., & Hayfron-Acquah, J. B. (2022). QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing), *International Journal of Computer Applications*, 184(33), 34-39.
- Arslan, M. (2011). Pazarlamada Kare Kod Kullanımı, *Bilim ve Teknik*, 44(738), 78-81.
- Bani-Hani, R. M., Wahsheh, Y. A., & Al-Sarhan, M. B. (2014). Secure QR Code System, *10th International Conference on Innovations in Information Technology*, 1-6.
- Başar, R. (2024). QR Kod İle Bir Siber Güvenlik Farkındalık Denemesi: Düzce Örneği. *Denetim*, 0(30), 214-225.
- Başaran, A., & Göksel, B. (2016). *QR Code'daki Olta Bir Farkındalık Deneyi ve QR Kodları Sosyal Mühendislik Saldırılarında Kullanılması*, <https://www.slideshare.net/slideshow/qr-codelardaki-tehlike/68516865> (17.10.2024)
- Bilir, M. O., & Özkoç, E. E. (2020). QR Kod Güvenlik Farkındalığı Üzerine Ankara İlinde Bir Araştırma, *İnternet Uygulamaları ve Yönetimi Dergisi*, 11(2), 113-129.
- Bozkurt, F., & Ergen, A. (2012). Pazarlama İletişiminde Yeni Bir Mobil Pazarlama Aracı: 2 Boyutlu Barkodlar, *Pazarlama ve Pazarlama Araştırmaları Dergisi*, 9, 43-64.
- Chen, F., Wong, K. Wo, Liao, X., & Xiang, T. (2014). Period Distribution of Generalized Discrete Arnold Cat Map, *Theoretical Computer Science*, 552, 13-25.
- Elçi, A. (2014). İş Ekipmanlarında Güvenlik Takibi İçin Bir Sistem Önerisi “Karekod Barkod Uygulama” (Yüksek Lisans Tezi). İstanbul Yeni Yüzyıl Üniversitesi, Sağlık Bilimleri Enstitüsü. <https://acikbilim.yok.gov.tr/handle/20.500.12812/702193>
- Ellerbee, S. M. (2009). An Artistic View of Posters, *Newborn and Infant Nursing Reviews*, 9(2), 109-110.
- Focardi, R., Luccio, F. L., & Wahsheh, H. A. M. (2019). Usable Security for QR Code, *Journal of Information Security and Applications*, 48.
- Goel, N., Sharma, A., & Goswami, S. (2017). A Way to Secure a QR Code: SQR. In *2017 International Conference on Computing, Communication and Automation*, 494-497.
- Hoy, M. B. (2011). An Introduction to QR codes: Linking Libraries and Mobile Patrons, *Medical Reference Services Quarterly*, 30(3), 295-300.
- Ismail, S., Alkawaz, M. H., & Kumar, A. E. (2021). Quick Response Code Validation and Phishing Detection Tool, In *2021 IEEE 11th Symposium on Computer Applications and Industrial Electronics*, 261-266.

- Kapsalis, I. (2013). *Security of QR Codes* (Master's thesis). Norwegian University of Science and Technology. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262814/644988_FULLTEXT01.pdf?sequence=2&isAllowed=y
- Kharraz, A., Kirda, E., Robertson, W., Balzarotti, D., & Francillon, A. (2014). Optical Delusions: A Study of Malicious QR Codes In the Wild, *Proceedings of the International Conference on Dependable Systems and Networks*, 192-203._
- Krombholz, K., Frühwirth, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR Code Security: A Survey of Attacks and Challenges for Usable Security, *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 79-90._
- Krombholz, K., Frühwirth, P., Rieder, T., Kapsalis, I., Ullrich, J., & Weippl, E. (2015). QR Code Security-How Secure and Usable Apps Can Protect Users Against Malicious QR Codes, *10th International Conference on Availability, Reliability and Security*, 230-237.
- Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental Investigation of Demographic Factors Related to Phishing Susceptibility, *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2240-2249.
- Liu, Z., Zhou, L., & Zhang, D. (2020). Effects of Demographic Factors on Phishing Victimization in the Workplace, *In PACIS*.
- Mahalakshmi, A., Goud, N. S., & Murthy, G. V. (2018). A Survey on Phishing and It's Detection Techniques Based on Support Vector Method (SVM) and Software Defined Networking (SDN), *International Journal of Engineering and Advanced Technology*, 8(2), 498-503.
- Moharil, B., Ghadge, V., Gokhale, C., & Tambvekar, P. (2012). An Efficient Approach for Automatic Number Plate Recognition System Using Quick Response Codes, *International Journal of Computer Science and Information Technologies*, 3, 5108-5115.
- Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which Phish Get Caught? An Exploratory Study of Individuals' Susceptibility to Phishing, *European Journal of Information Systems*, 26(6), 564-584.
- Örücü, A. İ. (2013). Bir Vergi Ödeme Aracı Olarak Karekod Teknolojisi, *Maliye Dergisi*, 0(164), 259-267.
- Piper, P. S. (2007). A Newer, More Profitable Aquaculture, *Searcher: Magazine for Database Professionals*, 15(9), 40-47.
- Pratama, A. R., Vadila, N., & Firmansyah, F. M. (2023). Exposing Generational and Gender Gap in Phishing Awareness Among Young Adults: A Survey Experiment, *AIP Conference Proceedings*, 2508(1).
- Sanal, A., & Öztürkoglu, Y. (2017). Hizmet Sektöründe QR Kod Kullanım Alanlarına Yönelik Bir Alan Çalışması, *Business & Management Studies: An International Journal*, 5(4), 172-189._

- Sharma, V. (2012). A Study of Malicious Qr Codes, *International Journal of Computational Intelligence and Information Security*, 3(5).
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.
- Shinde, S. S., Kale, G. M., Nalbalwar, S. L., & Deosarkar, S. B. (2024). Navigating the Cyber Battlefield: Understanding Threats and Safeguarding Digital Frontiers, *International Conference on Electrical Electronics and Computing Technologies*, 1, 1-6.
- Sun, A., Sun, Y., & Liu, C. (2007). The QR-Code Reorganization in Illegible Snapshots Taken by Mobile Phones, *Proceedings - The 2007 International Conference on Computational Science and Its Applications*, 532-536.
- Tarhan, K. (2022). Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies, *Przegląd Strategiczny*, 12(15), 393-414.
- Thamilvanan, G., & Mohanasundaram, K. (2019). Quick Response Code As a Communication Medium, *International Journal of Innovative Technology and Exploring Engineering*, 8(10), 4190-4192.
- Varshney, G., Misra, M., & Atrey, P. K. (2016). A Survey and Classification of Web Phishing Detection Schemes, *Security and Communication Networks*, 9(18), 6266-6284.
- Vidas, T., Owusu, E., Wang, S., Zen, C., & Cranor, L. (2012). QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks, *International Conference on Financial Cryptography and Data Security*, 52-69.
- Wahsheh, H., & Al-Zahrani, M. (2021). Secure Real-Time Computational Intelligence System Against Malicious QR Code Links, *International Journal of Computers, Communications and Control*, 16(3), 1-9.
- Webtekno. (2017). Çin Dolandırıcılığı Önlemek İçin QR-Kod Ödemelerini Durdurdu, <https://www.webtekno.com/cin-dolandiriciligi-onlemek-icin-qr-kod-odemelerini-durduruyor-h38598.html> (26.08.2024).
- Wen, L., Jingjing, W., Chen, W., & Luyu, S. (2022). Research on the Visual Imagery of Posters Based on the Culture Code Theory of Design, *Frontiers in Psychology*, 13.
- Yin, L. R., Senior, M., Zhang, Z., & Baldwin, N. (2013). Perceived Security Risks of Scanning Quick Response (QR) Codes in Mobile Computing with Smart Phones, *International Conference on Engineering, Management Science and Innovation*, 1-7.
- Yuwei, Y., & Su, Y. (2020). A Two-Dimensional Code Security Authentication Method Based on Digital Watermarking, *ACM International Conference Proceeding Series*, 94-99.
- Zhu, L. (2014). Security Protection Model of QR Code Scanning Software, *Advanced Materials Research*, 989, 4371-4374.