

Bireylerin İnternet-Dijital Cihaz Kullanım Becerilerini Değerlendirmelerinde Etkili Olan Faktörlerin Belirlenmesi¹

Determining the Factors Effective in Evaluating Individuals' Internet-Digital Device Usage Skills

Özlem KURU SÖNMEZ²

Emre YAKUT³

Araştırma Makalesi/ *Research Article*

Geliş Tarihi / Received: 12.04.2022

Kabul Tarihi / Accepted: 04.10.2022

Doi: 10.48146/odusobiad.1102997

Atıf / Citation: Kuru Sönmez, Ö. & Yakut, E., (2022). “Bireylerin İnternet-Dijital Cihaz Kullanım Becerilerini Değerlendirmelerinde Etkili Olan Faktörlerin Belirlenmesi” ODÜSOBİAD 12 (3), 2551-2578
Doi:10.48146/odusobiad.1102997

Öz

İnternet ve dijital cihaz kullanma (İDCK) becerisi Covid-19 salgınıyla artan uzaktan eğitim ve çalışma süreçleri nedeniyle bir zorunluluk haline gelmiştir. Artan internet ve dijital cihaz kullanımı ve dijital uçurumun etkisiyle siber suç mağduru olma riski artmıştır. Kurumlar ve kuruluşlar paydaşlarını çevrimiçi süreçler hakkında bilgilendirmek için çaba gösterebilirler bile uzaktan eğitim ve çalışma süreçleri hakkındaki deneyimsizlik olumsuz sonuçlar yaratmak için önemli bir etken olarak kendini göstermiştir. Bu sonucun bireylerin kendi internet ve dijital cihaz kullanım becerilerinin yeterli düzeyde olduğunu kabullenmesinden kaynaklanabileceği düşünülmektedir. Bu nedenle bireylerin kendi internet ve dijital cihaz kullanım becerisi hakkındaki düşüncelerini öğrenmek önem arz etmektedir. Bu çalışmada, bireylerin kendi İDCK beceri düzeyleri hakkındaki düşünceleri ve bu düşüncelerini etkileyen faktörler incelenmiştir. Osmaniye ilinde yaşayan 522 kişiye uygulanan anket aracılığıyla elde edilen verilere sıralı lojistik regresyon analizi ve marjinal etki analizi uygulanmıştır. Sonuçlara göre örnekleme yer alan 50 yaş üzerinde olan bireylerin, üniversite mezunu bireylerin, erkeklerin ve özel sektör çalışanı olan bireylerin İDCK becerisi açısından kendilerini diğerlerinden daha becerili görme eğiliminde olduğu belirlenmiştir. Ele alınan örneklem özelinde bireylerin kendi İDCK becerilerini değerlendirmelerinde etkili olan diğer faktörler, kullanılan işletim sistemleri, web sitesi kullanımında yasallık kontrolü yapma

¹ Bu çalışma, 8-10 Eylül 2021, 21. Uluslararası Ekonometri, Yöneylem Araştırması, İstatistik Sempozyumu'nda sözlü bildiri olarak (özet) sunulmuştur. Çalışmanın verilerinin edinilmesi için Osmaniye Korkut Ata Üniversitesi Sosyal Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu'na gerekli onay sağlanmıştır (Tarih: 10.01.2022, Sayı: 2022/1/4).

Çalışmanın araştırma ve yayın süreci, yayın etiğine uygun olarak yürütülmüştür. Anket formunun uygulanması için Osmaniye Korkut Ata Üniversitesi Sosyal Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu'ndan izin alınmıştır (Tarih: 10.01.2022, Sayı: 2022/1/4).

² Sorumlu yazar, Arş. Gör., Osmaniye Korkut Ata Üniversitesi, Osmaniye, E-mail: ozlemkuru@osmaniye.edu.tr, ORCID ID: 0000-0003-0208-4781

³ Doç. Dr., Osmaniye Korkut Ata Üniversitesi, Osmaniye, E-mail: emreyakut@osmaniye.edu.tr, ORCID ID: 0000-0002-1978-0217



sıklığı, eposta ve gönderilerdeki bağlantıların kontrolü, siber mağduriyet riskindeki artış farkındalığı ve devlet gözetimi kabulü olarak belirlenmiştir.

Anahtar Kelimeler İnternet Dijital Cihaz Kullanım Becerisi, Siber Güvenlik Faaliyeti, Siber Suç Bilinci, Sıralı Lojistik Regresyon

Abstract

The ability to use the Internet and digital devices (IDCK) has become a necessity due to the increasing distance education and working processes with the Covid-19. The risk of becoming a victim of cybercrime has increased due to the increasing use of internet and digital devices and the digital divide. Even though institutions and organizations make an effort to inform their stakeholders about online processes, lack of experience in distance education and working processes emerged as an important factor for creating negative results. It is thought that this result may be due to the fact that individuals accept that their internet and digital device usage skills are at a sufficient level. For this reason, it is important to learn the thoughts of individuals about their own internet and digital device usage skills. In this study, individuals' thoughts about their own IDCK skill levels and the factors affecting these thoughts were examined. Sequential logistic regression analysis and marginal effect analysis were applied to the data obtained through the questionnaire applied to 522 people living in Osmaniye. According to the results, it was determined that individuals over the age of 50, university graduates, men and individuals working in the private sector in the participants tend to see themselves as more skillful than others in terms of IDCK skills. Other factors that affect individuals' assessment of their own IDCK skills, specific to the sample discussed, were determined as the operating systems used, the frequency of legality checks in the use of the website, the control of links in e-mails and posts, the awareness of the increase in the risk of cyber victimization, and the acceptance of state surveillance.

Keywords Internet Digital Device Usage Skill, Cyber Security Activity, Cybercrime Awareness, Ordinal Logistic Regression

Giriş

Bireylerin internet ve dijital cihaz kullanma beceri düzeyleri arasındaki farklılıkları belirlemek için kullanılan dijital bölünme kavramı, ilk önceleri bilgisayar ve modem erişimi olan ve olmayan bireyler arasındaki eşitsizliklere dikkat çekmek üzere kullanılmışken sonradan bireysel internet kullanımına erişimdeki fırsat eşitsizliklerini açıklamak üzere vurgulanmıştır (NTIA, 1995;1998;1999). Benzer şekilde günümüzdeki tanımı, bilgi ve iletişim teknolojilerine erişim ve kullanım konusundaki eşitsizlik olarak kullanılmaktadır (Sezgin ve Fırat, 2020). Sosyal eşitsizlik türlerinden biri olan bu kavram; cinsiyet, coğrafi bölge, sosyal sınıf, yaş gibi özelleştirilebilecek coğrafi, kültürel, ekonomik, bilişsel ve nesiller arası farklılık gibi temellere dayanmaktadır (Mínguez ve Ballesteros, 2008; Pagani ve Pasinetti, 2009). Dijital bölünme nedeniyle ülke içinde bireylerin karşılaştıkları fırsat eşitsizlikleri, geniş anlamda

ülkeler arası haliyle de gündeme gelmektedir. Bilgi toplumu olarak adlandırılan, bilginin stratejik öneme sahip bir kaynak olarak değerlendirildiği ve teknolojinin öncülük ettiği bir değişim hareketinin hayatın her anında vazgeçilmez olduğunu açıklayan kavramın da etkisiyle dijital bölünme daha da önem kazanan bir tartışma konusu olmuştur (Çapar ve Vural, 2013; Ünal, 2009). Bu nedenle bireylerin hangi coğrafyada, hangi cinsiyetle, dünyaya ne zaman geldiğine ve nasıl bir kültürle büyüdüğüne bakılmaksızın bilgi iletişim teknolojilerine erişmeleri ve gerektiği zaman kullanabilmeleri önem arz etmektedir.

Dijital bölünme kavramının farklı tanımlarına ve içeriklerine göre dezavantajlı olabilecek özellikteki bazı gruplardan bahsetmek mümkündür. Örneğin yaş baz alındığında daha yaşlı olanlar gençlere göre, eğitim baz alındığında eğitim düzeyi az olanlar çok olanlara göre, gelir baz alındığında düşük gelirlilerin diğerlerine göre, cinsiyet baz alındığında kültüre göre değişkenlik göstermekle birlikte kadınların erkeklere göre, Türkiye'deki coğrafi bölgeler baz alındığında Güney ve Doğu Anadolu bölgelerindekilerin Marmara ve Karadeniz bölgelerindekilere göre dezavantajlı gruplarda olduğu anlaşılmıştır (Öztürk, 2005; Ağaoğlu, 2020). Açıklanan demografik özelliklerin yanı sıra dijital bölünmenin belirlenmesinde önemli olan diğer boyutlar teknik imkanlar, kullanım özerkliği, kullanım örüntüleri, sosyal destek ağları ve internet ve dijital cihaz kullanma beceri düzeyidir (Ağaoğlu, 2020). Beceri boyutunun içeriğinden internet ve dijital cihaz kullanım (İDCK) becerisi, kişiler ve kurumlar için hayatın her anında kendini gösteren, dijital dönüşüm nedeniyle giderek daha da önemli hale gelen bir ihtiyaçtır (Bayrakçı, 2020). Ancak bu ihtiyaç, 2019 yılının sonunda ortaya çıkan Covid-19 salgını ile birlikte tüm dünyada başta uzaktan eğitim ve uzaktan çalışma nedeniyle bir zorunluluk halini almıştır. Bu süreçte henüz yeterli altyapıya sahip olmayan kurumlarda bile çok kısa sürelerde acil uzaktan eğitim programı alternatifleri düzenlenip yüz yüze eğitime ara verilmiştir (Eken vd., 2020). Birçok şirket ve kamu kuruluşu, tüm paydaşları ve toplum sağlığını düşünerek uzaktan çalışma kararı almıştır. Bu nedenle kurumlar paydaşlarına bu süreçleri öğretmek için de ciddi bir emek sarf etmek durumunda kalmıştır. Birçok ülkede olduğu gibi Türkiye'de de uzaktan çalışma konusundaki deneyim eksikliği, diğer bir deyişle çalışanların uzaktan çalışma stiline ilk kez katılım sağlaması, uzaktan çalışmanın geçici bir önlem olarak görülüp benimsenememesine ve olumlu sonuçlar elde edilememesine neden olmuştur (İlhan, 2021: 341-342). Bunun yanı sıra Covid-19 sürecinde neredeyse tamamen dijital ortama taşınan iş ve eğitim süreçleri sebebiyle insanlar internet ve ekranlar karşısında çok fazla zaman geçirmeye başlamıştır. İlgili süreçte teknik ve mental altyapı anlamında uzaktan çalışma ve eğitim süreçlerine hazır olmayan paydaşların olduğu anlaşılmıştır (Özdoğan ve Berkant, 2020; Serinikli, 2021; Yılmaz, 2021: 181-183). Bu durum, interneti kötüye kullananlar için bir fırsat oluşturmuş ve bu süreçte normalden daha fazla siber suçların ortaya çıkmasına neden olmuştur (Sarıgedik, 2022; Seyran, 2021; Deniz ve Iriz, 2020). Ayrıca dijital bölünmenin siber zorbalığa ve dolayısıyla siber mağduriyete de katkı sağladığı bilinmektedir (Steinmetz, 2013: 42-46).

Çalışmada siber güvenlik faaliyetleri ve siber suç bilinci faktörlerinden bireylerin internet ve dijital cihaz kullanım beceri düzeylerini etkileyen faktörlerin neler olduğu araştırılmaktadır. Çalışmanın giriş bölümünden sonra ikinci kısmında araştırmanın kavramsal çerçevesi içerisinde internet ve dijital cihaz



kullanım becerisi, siber güvenlik faaliyeti, siber suç bilinci ve literatür açıklaması yapılmıştır. Çalışmanın üçüncü kısmında araştırmanın metodolojisi kapsamında ki-kare ve sıralı lojit model analizi uygulanarak bulgulardan bahsedilmiş, son bölümde ise tartışma ve sonuç kısmı yorumlanmıştır.

Kavramsal Çerçeve

İnternet ve Dijital Cihaz Kullanım Becerisi

İnternet ve dijital cihaz kullanım becerisi (İDCK), Bilgi ve İletişim Teknolojileri altyapısının gelişerek yangınlaşmasıyla beraber ortaya çıkarak önem kazanmıştır. Dijital cihaz kullanım becerisi, bilgiye ulaşmak ve bilgiyi yönetmek için gerekli olan cihazları ve internet uygulamalarını kullanmak için sahip olunması gereken yetenek olarak tanımlanmıştır (UNESCO, 2018). Benzer şekilde bireylerin internet ve bilgisayar kullanma becerisi, bu cihazları etkin kullanabilme ve bunlardan yeni bilgiler türetebilme becerileri olarak bahsedilmiştir (EUROSTAT, 2020). Bu tanımlardan hareketle, İDCK beceri seviyeleri cinsiyet, sektör, gelir, eğitim, bölge ve ülke açısından farklılık gösterebildiği için bu farklılıklar dijital bölünme veya dijital eşitsizliklerin belirlenmesinde kullanılmaktadır (Bozkanat ve Başol, 2021: 590). Başka bir ifadeyle Dijital bölünme veya dijital boşluk olarak da bilinen bu tanım, İngilizce’de digital divide, digital gap veya digital division olarak tanımlanmaktadır (Pierce, 2018 : 1).

İDCK beceri seviyelerindeki farklılıklar, bilim ve teknoloji alt yapısının her geçen gün hızla gelişmesine bağlı olarak ortaya çıkarken, bu durum kullanıcıların sahip olması gereken becerilerin farklılaşmasından kaynaklandığı görülmektedir (Yontar, 2019: 816; Şahin, Özkan ve Turan, 2022: 620). İDCK beceri düzeyindeki farklılıkların nedenleri arasında bireylerin eğitim seviyesi, gelir seviyesi, toplumun ilgili olması ve dijital okuryazarlık kapasitesi olarak sayılmaktadır (Kerman, Sönmez ve Kiraz, 2021: 61).

İDCK beceri düzeyindeki farklılaşmaya neden olan faktörler arasında literatür çalışmaları incelediğinde; sosyo-ekonomik faktörler, güvenlik faaliyetleri, siber zorbalık ve siber suç bilinci gibi faktörlerin etkili olduğu belirtilmektedir (Tekin, Süngü, Aydoğan ve Özer, 2022: 93). Bu çalışmada bireylerin İDCK beceri düzeylerine etki eden faktörlerden siber güvenlik faaliyetleri ve siber suç bilinci kavramları üzerinde durulacaktır.

Siber Güvenlik Faaliyeti

İDCK beceri düzeyine etki eden faktörlerden birisi olan siber güvenlik faaliyeti kapsamında öncelikle siber güvenlik kavramı açıklanmaya çalışılacaktır. Siber güvenlik; siber ortamda gerçekleştirilen bilişim sistemlerini saldırı ve tehlikeli faaliyetlerden korumak amacıyla, tehdit ve saldırıların önemini ve kaynaklarını tespit ederek bilgilerin gizliliğinin sağlanması, bunlara karşı yapılacak her türlü hukuka uygun önlemler ve tedbirler olarak tanımlanmaktadır (Atakan, 2021: 29). Başka bir ifadeyle siber güvenlik, bilişim sistemleri kapsamında değerlendirilen bilgisayar ve elektronik iletişim sisteminde kaydedilen bilgilerin doğruluğuna, gizliliğine ve kullanılabilirliğine erişim izni olmayan kişi veya

bunlara yönelik saldırılardan korumak için alınması gereken bir tür önlemlerdir (Akçakanat, Özdemir ve Mazak, 2021: 249).

Siber güvenlik faaliyetleri, iletişim altyapısı da dahil olmak üzere bireyler ve kurumların bilgi kaynaklarının siber saldırılara karşı korunması ve devamlı olarak güvende tutulması ile ilgili tüm çabalar olarak açıklanmaktadır (Karacı, Akyüz ve Bilgici, 2017). Başka bir ifadeyle, siber güvenlik faaliyetleri; bir bilişim sistemi içerisinde bilgilerin gizliliği, bütünlüğü ve ulaşılabilirliğini korumak olarak ifade edilmektedir (Kiraz, 2021: 72). Böylece siber güvenlik faaliyetleri bilişim sistemleri üzerinde bilginin gizlilik ilkesi, bütünlüğü kapsamında ve erişilebilirliği açısından üç kriterin sağlanmasıyla gerçekleştirilir (Çakır ve Uzun, 2021: 357).

Dijitalleşen dünyada internete bağlı insanların giderek artmasının sonucunda bu ortamda ciddi siber güvenlik risklerinin ortaya çıktığı ve bu nedenle siber güvenlik bilincinin güçlendirilmesi gerektiği ortaya çıkmıştır (Alzubaidi, 2021). Bireylerin internet ve dijital cihaz kullanımını konusundaki becerileri, etkileşimli ortamlarda güven altında kalmak, dijitalleşen topluma katılım sağlamak ve yaşam boyu öğrenme süreçlerinde aktif olabilmek için gereken ana yetkinliklerdendir (Bayrakçı, 2020). Literatürde uzun yıllardır tartışılan siber güvenlik ve bilgi güvenliği farkındalığı konularına dair birçok çalışmaya rastlamak mümkündür (Öztemiz ve Yılmaz, 2013; Erol vd., 2015; Keser ve Güldüren, 2015; Karacı, Akyüz ve Bilgici, 2017; Karaoğlu-Yılmaz ve Çavuş-Ezin, 2017; Talan ve Aktürk, 2021). Bu çalışmaların büyük kısmında bireylerin bilgi güvenliği konusundaki farkındalığı amaçlanmıştır.

Siber Suç Bilinci

Siber suç, yasa dışı olarak ifade edilen ve elektronik ortamda bilgisayarlar yardımıyla yapılan faaliyetlerdir (Thomas ve Loader, 2000:3). Siber suç kavramı, bilişim suçları anlamında kullanılmakta olup, bilişim sistemlerindeki verilerin hedef alınırken, bunların bilişim teknolojileri yardımıyla gerçekleştirildiği suçlar olarak açıklanmaktadır (Kuvancı ve Akın, 2020: 34). Başka bir ifadeyle, bilgisayarlar aracılığıyla bilgilerin bir sistemden başka bir yere taşınmasıyla kanuni ve ahlaki olmayan davranışlar ortaya çıkardığı; bu durumun hukuki, ahlaki, ekonomik ve toplumsal boyutunu içeren bir suç olduğu belirtilmektedir (Küçükvardar, 2018: 10).

Bilişim suçlarının içeriği, oldukça karmaşık suçlar olduğu, bu suçların birey, toplum ve devlete yönelik kanunlarla yasaklanmış faaliyetlerin kontrol mekanizmalarının yetersizliği nedeniyle gerçekleştirilerek bilişim alanında suç işlenmesine yol açtığı anlaşılmaktadır (Bahar, 2018: 3). Siber suçlar; geleneksel suçlar arasında yer alan dolandırıcılık ve sahtecilik suçların yanı sıra bilgi sistemlerine yönelik bir saldırı, hizmet dışı bırakma saldırısı olabildiği gibi kötücül bir yazılım ya da sosyal medya suçu da olabilmektedir (Aksoy ve Erilli, 2021: 241).

Teknolojik araçların gelişmesiyle siber suçluları her türlü teknolojik alt yapıdan faydalanmaktadır. Aynı zamanda, bireylerin internette geçirdiği zaman, günlük hayatlarında gerçekleştirdikleri alışveriş, iletişim, eğitim ve hatta çalışma hayatı gibi birçok eylemin internete taşınması ile son derece artarken, bu durum siber suçlular için fırsatlar oluşturmaktadır. İnternette gerçekleştirilen eylemlerin anonim olabilmesi, takibinin teknik uzmanlık gerektirebilmesi veya geliştirilmeye devam eden ceza ve adalet



sistemi nedeniyle siber suç mağduru olma riski artmıştır. Ancak internet ortamında bireyler karşı karşıya oldukları durumun bir siber suç faaliyeti olduğunu, çevrim içi ve çevrim dışı suçların ayrımını, çevrim içi ortamda suç olarak tanımlanan faaliyetlerin sınırlarını fark etmek konusunda sorunlar yaşayabilmektedirler (Karagiannopoulos, Kirby ve Sugiura, 2021). Bu durum "Cybercrime Awareness" olarak anılan siber suç bilinci kavramı, bireylerin bilgi ve iletişim teknolojileri destekli suçları algılayabilme düzeyiyle açıklanmaktadır (Nzeakor, Nwokeoma ve Ezech, 2020; Zayif ve Farah, 2017; Ismailova ve Muhametjanova, 2016).

Günümüzde gelişen teknolojiler ve ortaya çıkan farklı bilişim araçları nedeniyle kullanıcılar yetersiz bilgi düzeyi, tutum ve davranışları sebebiyle siber suçlara karşı savunmasız olduğu belirlenirken, bu anlamda siber tehditleri önleme ve etkisini azaltmanın yöntemlerinden birisi olarak bireysel ya da kurumsal anlamda siber suç bilincini oluşturmak amacıyla kullanıcılara eğitimler verilmesi ihtiyaç haline gelmiştir (Öğün ve Kaya, 2013; Altınöz, Tosun, Çinkılıç ve Çay, 2019: 2).

Literatür Taraması

Dijital bölünmenin belirlenmesinde kullanılan boyutlardan birisi olan İDCK becerisiyle ilgili çalışmaların yeterli sayıda olmayışından literatür çalışması bireylerin İDCK beceri düzeylerini kapsayacak şekilde dijital bölünmeyi araştırma konusu alan çalışmalar üzerinde özetlenmeye çalışılmıştır.

Kalaycı (2011), gelişmiş ve gelişmekte olan ülkelerin 2011 yılına ait dijital bölünme, dijital yoksulluk ve uluslararası ticaret endeks değerlerini oluşturan gösterge değerlerini kullanarak grafiklerle yorumlamaya çalışmıştır. Araştırmada ülkelerin dijital yoksulluk gibi dijital bölünme endeksinin azaldıkça toplumun refahını olumsuz yönde etkileyen unsurlar olduğunu açıklamıştır.

Baran, Kurt ve Tekeli (2017), TÜİK'in 2016 yılı Hane halkı Bilişim Teknolojileri Kullanım Araştırması veri setini kullanarak 60-74 yaş aralığındaki bireylerin dijital teknolojileri kullanım düzeylerini değerlendirmek için varyans analizi uygulamışlardır. Çalışma sonucunda yaşlı bireylerin bilişim teknolojilerine hakim olduklarını belirtirken demografik unsurların İDCK beceri düzeyleri üzerinde etkili olduğunu açıklamışlardır.

Erten (2019), Türkiye ve dünyadaki ülkelerin 2016 ve 2017 yılı bilgi ve iletişim teknolojileri endeksi verilerini kullanarak ülkeler arasında karşılaştırma yapmaya çalışmıştır. Araştırmada Türkiye'de dijital bölünme sorunu olduğunu vurgulayarak devlet ve özel kurumlara gerekli önlemlerin alınması konusunda uyarılarda bulunmuştur.

Yontar (2019), bir devlet üniversitesinin sosyal bilgiler eğitimi bölümünde okuyan 216 öğretmen adayına dijital bölünmenin boyutlarından olan dijital okuryazarlık düzeylerini değerlendirmek için anket uygulamıştır. Araştırma sonucunda katılımcıların dijital okuryazarlık düzeylerinin orta düzeyde olduğunu, erkeklerin kadınlara kıyasla bu düzeyin anlamlı derecede yüksek olduğunu vurgulayarak öğretmen adayları arasında dijital bölünme sorunu olduğunu belirtmiştir.

Aksoy, Karabay ve Aksoy (2021), Türkiye'nin farklı illerinde görev yapan 329 sınıf öğretmenine anket uygulayarak dijital bölünmeyi belirlemede kullanılan dijital okuryazarlık seviyelerini demografik özelliklere göre kıyaslamaya çalışmışlardır. Araştırma sonucunda öğretmenlerden lisansüstü eğitim seyisine sahip olanların ve daha düşük yaşta olanların dijital okuryazarlık düzeylerinin arttığı buna karşın cinsiyet ve dijital cihaz kullanım süreleri açısından anlamlı bir farklılaşma olmadığı sonucuna ulaşmışlardır.

Alvarez ve García-Prieto (2021), Covid 19 sürecinde İspanya'nın kırsal bölgesindeki okulların karantina ve uzaktan eğitim gibi süreçlerden nasıl etkilendiğini belirlemeye çalışmışlardır. Çalışma sonucunda incelenen örneklemin %30'unda dijital bölünme probleminin yaşandığını vurgulamışlardır.

Alzubaidi (2021), Suudi Arabistan'da 1230 kişiye gerçekleştirdiği çevrimiçi anket aracılığıyla bireylerin siber güvenlik faaliyeti ve siber suç bilinci farkındalığını belirlemeyi amaçlamıştır. Araştırma sonucunda katılımcıların %31,7'sinin İnternet için Wi-Fi kullandığını belirttikleri, %51'inin parola oluşturmak için kişisel bilgilerini kullandığını açıkladıklarını, %32,5'inin kimlik avı saldırıları hakkında hiçbir fikrinin olmadığını ifade ettikleri, %21,7'sinin siber suçların kurbanı olduğunu söylemişlerdir. Çalışma sonucunda siber suçlara önlenmesine yönelik önerilerde bulunmuştur.

Bozkanat ve Başol (2021), 2017 yılı 28 AB üyesi ülkelerin bireylerin dijital becerilerinin toplumsal cinsiyet eşitsizliği indeksi üzerinde etkili olup olmadığını belirlemek için seçilen verilere yapısal eşitlik modeli analizini uygulamışlardır. Çalışma sonucunda bireylerin yüksek dijital becerilerinin toplumsal cinsiyet eşitliği indeksini iyileştirdiği sonucuna ulaşmışlardır.

Elena-Bucea, Cruz-Jesus, Oliveira, & Coelho (2021), AB üyesi 28 ülkenin 2016 yılı verilerini kullanarak ülkelerin dijital bölünme sıkıntısını etkileyen faktörleri belirlemek için faktör analizi, varyans analizi, rank testi analizi gerçekleştirmişlerdir. Çalışma sonucunda dijital bölünme üzerinde e-hizmetler faktörü altında eğitim düzeyinin ve sosyal ağlar faktörü altında ise bireyin yaşının daha fazla etkili olduğu sonucuna varmışlardır.

Nandal, Singla ve Rawal (2021), Covid 19 sürecinde Hindistan'da eğitim sisteminin çevrimiçi eğitime geçilmesinin etkileri ve dijital bölünmeyi araştırmışlardır. Çalışmada 500 kişiye gerçekleştirdikleri anket verilerine ki-kare analizi ve lojistik regresyon analizi uygulayarak örneklemin %42'sinde dijital bölünme sıkıntısının olduğunu tespit etmişlerdir.

Uyar ve Taşdemir (2021), Ankara'daki ortaokula devam eden 1453 öğrenciye anket uygulayarak çocukların internete erişim ve kullanım becerilerini değerlendirmeye çalışmışlardır. Çalışma sonucunda ailenin sosyoekonomik düzey farklılıkları ve eğitim düzeyi ile çocukların İDCK beceri düzeyleri arasında bir ilişkili olduğu sonucuna varmışlardır.

Wang, Zhou ve Wang (2021), Çin'deki bilgi ve iletişim teknolojileri (BİT) kullanımı ve dijital bölünmenin kentleşme üzerinde bir etkisinin olup olmadığını temel bileşenler analizi, yapısal eşitlik modeli ve coğrafi ağırlıklı regresyon yöntemleriyle belirlemeye çalışmışlardır. Araştırma sonucunda BİT



kullanımının kentleşmeyi olumlu etkilerken dijital bölünmenin kentleşmeyi olumsuz etkilediği sonucuna varmışlardır.

Dağlı (2022), Türkiye’de Düzey1’deki 12 bölge üzerinden 2011-2021 yılına ait verileri kullanarak dijital bölünmenin durumunu çok kriterli karar verme tekniklerinden EDAS ve MAIRCA tekniklerini kullanarak değerlendirmeye çalışmıştır. Araştırma sonucunda on yıl öncesiyle kıyaslandığında bölgeler açısından büyük oranda dijital bölünme değişimi yaşanmadığını, 2021 yılı verileri incelendiğinde bölgelere yönelik dijital bölünme sıralamasında ilk sırada İstanbul bölgesinin son sırada ise Kuzeydoğu Anadolu bölgesinin yer aldığını tespit etmiştir.

Güner (2022), AB üye ülkelerin 2019 yılı dijital okuryazarlık düzeylerini karşılaştırmak için ülkeler açısından bireylerin dijital beceri düzeyleriyle açıklamaya çalışmışlardır. Araştırma sonucunda dijital beceri düzeyleri yüksek olan kuzeydeki gelişmiş ülkelerin doğu bölgesindeki ülkelere kıyasla dijital okuryazarlık sıralamalarının daha iyi olduğu sonucunu vurgulamışlardır.

Kuh ve Erdem (2022), Türkiye’nin Batı Akdeniz bölgesinde yaşayan 450 katılımcıya anket uygulayarak dijital bölünmenin sağlık hizmetleri kullanımı üzerine etkisinin olup olmadığını çoklu regresyon analiziyle belirlemeye çalışmışlardır. Analiz sonucunda katılımcıların BİT bilgi düzeyi arttıkça dijital sağlık uygulamalarına yönelik bilgi düzeylerinin arttığını belirlemişlerdir.

Tekin, Süngü, Aydoğan ve Özer (2022), Pandemi sürecinde engelli birey ve annelerin yaşam kaliteleri üzerine bir değerlendirme gerçekleştirmek için soru formu oluşturarak katılımcıların görüşlerini almışlardır. Yapılan değerlendirme sonucunda çevrimiçi destek eğitim hizmetleri imkanı bulunmayan bireylerin fırsat eşitliğinden yararlanamadığını, bu durumun dijital bölünmeye yol açtığını vurgulayarak ekonomik anlamda yetersiz olan bireylere teknolojik ürün ve internet imkanlarının sunulması gerektiğini açıklamışlardır.

Araştırmanın Amacı ve Yöntemi

Araştırmadaki amaç, siber güvenlik faaliyetleri ve siber suç bilinci faktörlerinden bireylerin internet ve dijital cihaz kullanım beceri düzeylerini etkileyen faktörleri tespit etmektir. Bireylerin demografik özellikleri, siber güvenlik faaliyetleri ve siber suç bilinci faktörleri ile İDCK beceri düzeyleri arasındaki ilişkinin anlamlı olup olmadığı tespit edilerek, anlamlı olan faktörlerin etki düzeyleri hesaplanarak yorumlanacaktır.

Çalışmada anket yoluyla elde edilen verilerinin frekansları, yüzdeleri hesaplanmış, bağımlı değişken olan İDCK becerisi ile bağımsız değişkenler arasındaki ilişki incelenmek üzere Pearson ki-kare analizi uygulanmıştır. Bu analizler için SPSS 18 paket programı kullanılmıştır. Pearson ki-kare analizlerinin sonuçlarına göre sıralı lojistik regresyon modeline dahil edilecek değişkenler belirlenmiş ve çoklu doğrusal bağlantı testi gerçekleştirilmiştir. Çoklu doğrusal bağlantı testi sonucunda elde edilen sonuçları eşik değerlerin altında olan değişkenler ile sıralı lojistik regresyon analizi gerçekleştirilmiştir.

Lojistik regresyon analizi yönteminde kategorik değişkenlerin sayısı ve bu kategorilerin nominal (sırasız olması) ve ordinal (sıralı olması) durumuna göre farklı türde lojistik regresyon yöntemleri uygulanmaktadır. Bağımlı değişkenin iki kategorili olması durumunda binary lojistik regresyon, ikiden çok kategori olması durumunda multinominal lojistik regresyon, ikiden çok sıralı kategori olması durumunda sıralı lojistik regresyon analiz yöntemi kullanılmaktadır (Kalaycı, 2010; Alpar, 2013; Alkan ve Abar, 2020; Yakut, 2020). Bu çalışmada Sıralı lojistik regresyon analizi sonrasında bağımsız değişkenlerin İDCK becerisinin olasılığına etkilerini belirlemek için marjinal etki analizi uygulanmıştır. Sıralı lojistik regresyon ve marjinal etki analizi için Stata 14 paket programı kullanılmıştır.

Araştırmanın Örneklemi ve Değişkenlerin Tanımlanması

Sosyal bilimlerde yapılacak olan çalışmalarda 1 milyon birime kadar evren büyüklüğünde 0.95 güven aralığında, %5'lik hata payı ile örneklem en az 384 birimden oluşmalıdır (Sekaran, 2003). Araştırmanın evrenini Osmaniye'de yaşayan 18 yaş üstü bireyler oluşturmaktadır.

Örnekleme yöntemleri temelde rastlantısal yöntemler ve rastlantısal olmayan yöntemler olarak iki grupta incelenmektedir. Rastlantısal olmayan örnekleme yöntemleri başlığı altında yer alan kolayda (gelişigüzel) örnekleme yöntemi ile belirlenen evrendeki seçilme şansı eşit olmayan örneklerden herhangi bir liste gözetilmeden seçilmesi ile uygulanır (Kılıç, 2013). Bu çalışmada Osmaniye'de yaşayan 18 yaş ve üzeri bireylerden rastlantısal olmayan örnekleme yöntemlerinden kolayda örnekleme yöntemi kullanılarak ulaşılanlara sunulan online anket uygulamasına katılan 522 kişinin cevapları çalışmanın veri seti olarak kullanılmıştır. Katılımcılara Osmaniye Korkut Ata Üniversitesi çalışanları ve öğrencileri, il genelinde çalışmalarını sürdüren sanayi ve imalat kuruluşlarında çalışan personeller ve bu grupların sosyal çevrelerinden ulaşılmıştır.

Anket formunda bireylerin temel demografik özelliklerini belirleyen cinsiyet, yaş, eğitim, istihdam durumu soruları ile birlikte Alzubaidi (2021) tarafından tasarlanan Bilgi Güvenliği Farkındalığı Ölçeği'nin Siber Güvenlik Faaliyetleri ve Siber Suç Bilinci bölümlerindeki ifadeler kullanılmıştır. Alzubaidi (2021) tarafından tasarlanan ölçekte kişisel bilgiler, siber güvenlik faaliyetleri, siber suç bilinci ve vaka raporları olmak üzere dört bölüm ve toplamda 62 ifade bulunmaktadır. İlgili ifadelerden ki-kare analizi sonucunda anlamlı olup sıralı lojistik regresyon analizine dahil edilenler ve bunların yanıt kategorileri Tablo 2'de gösterilmiştir. Çalışmada bireylerin kendi internet ve dijital cihaz kullanım becerilerini değerlendirdikleri internet ve dijital cihaz kullanım beceri düzeyi (İDCK) değişkeni bağımlı değişken olarak belirlenmiştir. Bireyler kendi becerilerini üç düzey üzerinden (Başlangıç: 1, Orta: 2 ve Uzman: 3) değerlendirmişlerdir.

Araştırmanın Modeli

Çalışmada literatür incelemesi doğrultusunda, bireylerin İDCK beceri düzeyleri üzerinde etkili olan faktörler belirlenmeye çalışılmıştır. Bu kapsamda kullanıcıların İDCK beceri düzeyi ile siber güvenlik faaliyeti ve siber suç bilinci arasındaki ilişkiyi tespit etmek için Ki-kare analizi gerçekleştirilmiş, sonrasında etkili olan faktörlerin sıralı lojistik regresyon modeliyle marjinal etkileri hesaplanmıştır.



Araştırma Hipotezlerinin Geliştirilmesi

Bireylerin internet ve dijital cihaz kullanma beceri düzeyleri arasındaki farklılıkları belirlemede kullanılan dijital bölünme kavramı; cinsiyet, sosyoekonomik durum, etnik köken ve coğrafya gibi farklı demografik özelliklere sahip bireyler arasında farklılık göstermektedir (Scheerder, Van Deursen, & Van Dijk, 2017). Blank ve Groselj (2014), yaptıkları çalışmada yaş, eğitim seviyesi ve istihdam durumunun dijital bölünmedeki farklılıkların büyük bir kısmına neden olduğunu açıklamışlardır. Siber ortamda gerçekleştirilen tehdit ve saldırıların önemi ve buna karşılık önlem ve tedbirleri kapsayan siber güvenlik faaliyetinin internet kullanımını üzerinde etkili olduğu ve görme engelli bireylere yaptıkları çalışmada siber güvenlik konusunda daha bilgili ve yetenekli olan kullanıcıların daha az bilgili olanlara göre daha fazla endişe duydukları ve dijital bölünme kavramı içerisinde değerlendirilen interneti kullanma konusunda daha az kullanma eğiliminde olduklarını ortaya koymuşlardır (Inan, Namin, Pogrud, ve Jones, 2016). Bilişim suçları bilgisi anlamına gelen siber suç bilinci, bireylerin internet ortamında bilişim sistemleri güvenliğinin sağlanmasına ve siber olayların etkilerinin düşük seviyede olmasına yardımcı olmaktadır (Gözler ve Taşçı, 2015). Alzubaidi (2021), Arabistan'da gerçekleştirdikleri çalışmada bireylerin siber suç farkındalık düzeyi arttıkça interneti daha güvenli kullandıkları, olası suçlara karşı daha bilinçli ve önleyici tutum sergileme seviyesinde olduklarını açıklamıştır. Siber suç farkındalık düzeyi ile internet kullanıcıların cinsiyet, yaş ve eğitim seviyeleri arasında ilişki olduğunu ortaya koyan çalışmalarda mevcuttur (Ndubueze, Igbo ve Okoye, 2013; Nzeakor, Nwokeoma ve Ezeh, 2020). Bu doğrultuda çalışmanın hipotezleri oluşturulmuş ve şu şekilde açıklanmıştır (Alzubaidi, 2021; Scalán, 2021; Tekin vd., 2022:93):

H₁: Bireylerin cinsiyeti ile İDCK beceri düzeyleri arasında ilişki vardır.

H₂: Bireylerin yaşı ile İDCK beceri düzeyleri arasında ilişki vardır.

H₃: Bireylerin eğitim seviyesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₄: Bireylerin istihdam durumu ile İDCK beceri düzeyleri arasında ilişki vardır.

H₅: Kullanılan bilgisayar işletim sistemi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₆: Kullanılan mobil işletim sistemi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₇: Cihazların ne kadar güvenli olduğu düşüncesi ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₈: Web sitelerine girmeden önce yasal olup olmadıklarını kontrol ederim ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₉: Şifrelerimi kişisel bilgilerimi kullanarak oluştururum ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₀: Tıkladığım reklamlardaki tehlikelerin farkındayım ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₁: Önemli hesaplarımın şifrelerini sıklıkla değiştiririm ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₂: Kullandığım yazılımları/uygulamaları düzenli olarak güncellerim ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₃: Bir e-posta veya gönderideki bağlantılara tıklarken dikkat ederim ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₄: Geçen yıla kıyasla siber suç mağduru olma riskinin arttığını düşünüyorum ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

H₁₅: İnternette güvenliğin artması koşuluyla devlet gözetiminin artmasını kabul ederim ifadesi ile İDCK beceri düzeyleri arasında ilişki vardır.

Betimleyici İstatistikler

Katılımcıların demografik bilgileri ile ilgili frekanslar ve yüzdeler Tablo 1’de sunulmuştur. Ayrıca katılımcıların İDCK becerisi ile bağımsız değişkenler arasındaki ilişkinin belirlenebilmesi için gerçekleştirilen Pearson ki-kare testinin sonuçları da ilgili tabloda aktarılmıştır. Demografik özelliklerin tamamının ki-kare testi sonuçları anlamlı bulunmuş ($p < 0.05$); H₁, H₂, H₃ ve H₄ hipotezleri kabul edilmiştir. Böylece bu değişkenlerin sıralı lojistik regresyon analizine dahil edilmelerine karar verilmiştir.

Tablo 1. Katılımcıların demografik özelliklerinin frekansları ve yüzdeleri

Değişken	BD: Başlangıç (n=118)	BD: Orta (n=311)	BD: Uzman (n= 93)	Tüm gözlemler (N=522)	Ki-Kare Testi
Cinsiyet					0.000 ^a
Kadın	85 (%72.0)	188 (%60.5)	36 (%38.7)	309 (%59.2)	
Erkek	33 (%28.0)	123 (%39.5)	57 (%61.3)	213 (%40.8)	
Yaş					0.038 ^b
18-29	99 (%83.9)	254 (%81.7)	82 (%88.1)	435 (%83.3)	
30-39	16 (%13.6)	36 (%11.6)	4 (%04.3)	56 (%10.7)	
40-49	1 (%00.8)	15 (%04.8)	2 (%02.2)	18 (%03.5)	
50+	2 (%01.7)	6 (%01.9)	5 (%05.4)	13 (%02.5)	
Eğitim Seviyesi					0.000 ^a
İlkokul-Ortaokul, Lise	34 (%28.8)	32 (%10.3)	2 (%02.1)	68 (%13.0)	
Ön lisans	12 (%10.2)	30 (%09.6)	14 (%15.1)	56 (%10.7)	
Lisans, Lisansüstü	72 (%61.0)	249 (%80.1)	77 (%82.8)	398 (%76.3)	
İstihdam Durumu					0.000 ^a
Kamu çalışanı	13 (%11.0)	35 (%11.2)	3 (%03.2)	51 (%09.7)	
Özel sektör çalışanı	17 (%14.4)	49 (%15.8)	33 (%35.5)	99 (%19.0)	
Çalışmıyor	88 (%74.6)	227 (%73.0)	57 (%61.3)	372 (%71.3)	

^a: $p < 0.000$, ^b: $p < 0.05$

Tablo 1’e göre katılımcıların %83.3’ü 18-29 yaş arasında, %59.2’si kadın, %76.3’ü lisans ve lisansüstü mezunu ve %71.3’ü çalışmayan bireylerdir. Katılımcıların bilgi güvenliği farkındalıkları hakkında etkili olan değişkenlerin frekans ve yüzdeleri Tablo 2’de sunulmuştur. Ayrıca bu değişkenlerden sıralı lojistik



regresyon analizine dahil edilecek olanları belirlemek üzere uygulanan ki-kare testinin sonuçları da ilgili tabloda sunulmuştur.

Tablo 2'ye göre beceri düzeyini başlangıç olarak değerlendirenlerin %20.34'ünün bilgisayar kullanmadığı, %2.54'ünün de kullandığı bilgisayar işletim sistemini bilmediği; beceri düzeyini orta olarak değerlendirenlerin ise %6.11'inin bilgisayar kullanmadığı ve %1.6'sının kullandığı bilgisayar işletim sistemini bilmediği anlaşılmıştır. Uzman düzeyde olduğunu belirtenlerden 1 kişinin bilgisayar kullanmadığı ve geri kalanların tamamının kullandığı bilgisayar işletim sistemini bildiği görülmektedir.

Mobil işletim sistemi değişkenindeki frekanslar incelendiğinde; İDCK becerisi başlangıç olanlardan %1.69'u, İDCK becerisi orta olanlardan %1.93'ü ve İDCK becerisi uzman olanlardan %1.08'i kullandığı mobil işletim sistemini bilmemektedir. Katılımcıların cihazlarının güvenlik düzeyi hakkındaki düşünceleri incelendiğinde; İDCK becerisi başlangıç olanlardan %30.51'i, İDCK becerisi orta olanlardan %26.36'sı ve İDCK becerisi uzman olanlardan %35.5'i cihazlarının güvenli olmadığını düşündüklerini belirtmişlerdir.

Katılımcıların web sitelerine girmeden önce yasal olup olmadıklarını kontrol etme davranışları incelendiğinde %50.96'sının sıklıkla kontrol ettiği, %17.43'ünün ise asla kontrol etmediği görülmektedir. Şifrelerinde kişisel bilgilerini sıklıkla-hep kullanan katılımcıların oranı %35.63 iken şifrelerinde asla kişisel bilgilerini kullanmadığını belirten katılımcıların oranı %39.08'dir. Tıklanan reklamlardaki tehlikelerin sıklıkla-hep farkında olduğunu belirten katılımcıların oranı %78.9 iken, tıkladığı reklamlardaki tehlikelere dair farkındalığına asla-nadiren şeklinde yanıt veren katılımcıların oranı %6.89'dur.

Kullandıkları hesaplardan önemli olanların şifrelerini sıklıkla değiştiren katılımcılar örneklemin %52.5'ini, asla şifre değiştirmedini belirten katılımcılar ise %17.6'sını oluşturmaktadır. Kullandıkları yazılımların güncellemelerini sıklıkla-hep düzenli olarak gerçekleştiren kullanıcılar örneklemin %68.77'sini ve güncellemelerini hiç düzenli olarak gerçekleştirilmeyen veya nadiren düzenli gerçekleştiren katılımcılar %8.62'sini oluşturmaktadırlar. Bir e-posta veya gönderi aldığı anda içerdiği bağlantılara tıklarken sıklıkla-hep dikkatli olduğunu belirten kullanıcıların %74.91, asla dikkat etmediğini veya nadiren dikkat ettiğini belirten kullanıcılar ise %7.66 orana sahip olduğu belirlenmiştir.

Tablo 2. Katılımcıların internet-dijital cihaz kullanım beceri düzeyini etkileyen değişkenlerin frekansları

Değişken	Beceri Düzeyi: Başlangıç (n=118)		Beceri Düzeyi: Orta (n=311)		Beceri Düzeyi: Uzman (n= 93)		Tüm gözlemler (N=522)		Ki-Kare Testi
Hangi bilgisayar işletim sistemini kullanıyorsunuz?									0.000 ^a
Windows	90	(%76.27)	283	(%91.00)	80	(%86.02)	453	(%86.78)	
MacOs	1	(%00.85)	4	(%01.29)	2	(%02.15)	7	(%01.34)	
Linux	0	(%00.00)	0	(%00.00)	10	(%10.75)	10	(%01.92)	
Bilmiyor	3	(%02.54)	5	(%01.60)	0	(%00.00)	8	(%01.53)	
Kullanmıyor	24	(%20.34)	19	(%06.11)	1	(%01.08)	44	(%08.43)	
Hangi mobil işletim sistemini kullanıyorsunuz?									0.033 ^b
Windows	8	(%06.78)	11	(%03.54)	5	(%05.38)	24	(%04.60)	
Blackberry	1	(%00.85)	0	(%00.00)	2	(%02.15)	3	(%00.57)	
Android	91	(%77.12)	209	(%67.20)	61	(%65.59)	361	(%69.16)	
iOS	16	(%13.56)	85	(%27.33)	24	(%25.81)	125	(%23.95)	
Bilmiyor	2	(%01.69)	6	(%01.93)	1	(%01.07)	9	(%01.72)	
Cihazlarınızın ne kadar güvenli olduğunu düşünüyorsunuz?									0.002 ^b
Güvenli Değil	36	(%30.51)	82	(%26.36)	33	(%35.50)	151	(%28.93)	
Kararsızım	62	(%52.54)	155	(%49.84)	27	(%29.00)	244	(%46.74)	
Güvenli	20	(%16.95)	74	(%23.80)	33	(%35.50)	127	(%24.33)	
Web sitelerine girmeden önce yasal olup olmadıklarını kontrol ederim.									0.000 ^a
Asla-Nadiren	31	(%26.27)	54	(%17.4)	6	(%06.45)	91	(%17.43)	
Bazen	34	(%28.81)	110	(%35.4)	21	(%22.58)	165	(%31.61)	
Sıklıkla-Hep	53	(%44.92)	147	(%47.3)	66	(%70.97)	266	(%50.96)	
Şifrelerimi kişisel bilgilerimi kullanarak oluştururum.									0.025 ^b
Asla-Nadiren	33	(%27.97)	125	(%40.20)	46	(%49.46)	204	(%39.08)	
Bazen	35	(%29.66)	80	(%25.72)	17	(%18.28)	132	(%25.29)	
Sıklıkla-Hep	50	(%42.37)	106	(%34.08)	30	(%32.26)	186	(%35.63)	
Tıkladığım reklamlardaki tehlikelerin farkındayım.									0.004 ^b
Asla-Nadiren	15	(%12.71)	16	(%05.14)	5	(%05.37)	36	(%06.89)	
Bazen	23	(%19.49)	44	(%14.15)	7	(%07.53)	74	(%14.18)	
Sıklıkla-Hep	80	(%67.80)	251	(%80.71)	81	(%87.10)	412	(%78.93)	
Önemli hesaplarımın şifrelerini sıklıkla değiştiririm.									0.043 ^b
Asla-Nadiren	24	(%20.34)	60	(%19.29)	8	(%08.60)	92	(%17.62)	
Bazen	38	(%32.20)	94	(%30.23)	24	(%25.81)	156	(%29.89)	
Sıklıkla-Hep	56	(%47.46)	157	(%50.48)	61	(%65.59)	274	(%52.49)	
Kullandığım yazılımları/uygulamaları düzenli olarak güncellerim.									0.000 ^a
Asla-Nadiren	18	(%15.25)	24	(%07.72)	3	(%03.23)	45	(%08.62)	
Bazen	39	(%33.05)	69	(%22.19)	10	(%10.75)	118	(%22.61)	
Sıklıkla-Hep	61	(%51.70)	218	(%70.09)	80	(%86.02)	359	(%68.77)	
Bir e-posta veya gönderideki bağlantılara tıklarken dikkat ederim.									0.000 ^a
Asla-Nadiren	15	(%12.71)	21	(%06.75)	4	(%04.30)	40	(%07.66)	
Bazen	31	(%26.27)	56	(%18.01)	4	(%04.30)	91	(%17.43)	
Sıklıkla-Hep	72	(%61.02)	234	(%75.24)	85	(%91.40)	391	(%74.91)	
Geçen yıla kıyasla siber suç mağduru olma riskinin arttığını düşünüyorum.									0.006 ^b
Katılmıyorum	7	(%05.93)	3	(%00.96)	3	(%03.22)	13	(%02.49)	
Kararsızım	21	(%17.80)	38	(%12.22)	7	(%07.53)	66	(%12.64)	
Katılıyorum	90	(%76.27)	270	(%86.82)	83	(%89.25)	443	(%84.87)	
İnternette güvenliğin artması koşuluyla devlet gözetiminin artmasını kabul edebilirim.									0.025 ^b
Katılmıyorum	23	(%19.49)	54	(%17.36)	29	(%31.18)	106	(%20.31)	
Kararsızım	34	(%28.81)	72	(%23.15)	16	(%17.20)	122	(%23.37)	
Katılıyorum	61	(%51.69)	185	(%59.49)	48	(%51.62)	294	(%56.32)	

a: p<0.000. b: p<0.05

Katılımcılardan İDCK becerisi başlangıç olanların %67.8'i, İDCK becerisi orta olanların %81.4'ü ve İDCK becerisi uzman olanların %81.7'si internet koruması kullandığını belirtmiştir. İnternet korumasını güncel tutma durumu incelendiğinde kullanan katılımcıların %96.1'inin internet korumasını güncel tutmaya dikkat ettikleri ve %3.9'unun internet korumasını güncel tutmaya dikkat



etmedikleri anlaşılmıştır. Siber suç mağduru olma riskinin geçen yıla kıyasla daha fazla olduğuna katılan kişiler örneklemin %84.9'unu, bu konuda kararsız olan kişiler %12.6'sını, katılmayan kişiler ise %2.5'ini oluşturmaktadırlar. "İnternette güvenliğin artması koşuluyla devlet gözetiminin artmasını kabul edebilirim" ifadesine katılanlar örnekleme %56.32'lik orana sahipken, katılmayanlar %20.31'lik orana sahiptirler.

"Siber suç tehdidi ile ilgili bilgilendirildiğimi hissediyorum" ifadesine katılma durumlarına göre katılımcılar incelendiğinde İDCK beceri düzeyi uzman olanlardan %57'sinin, orta olanlardan %40.5'inin ve başlangıç olanlardan %36.4'ü ifadeye katılıyorken; İDCK beceri düzeyi uzman olanlardan %19.4'ünün, orta olanlardan %35.4'ünün ve başlangıç olanlardan %36.4'ünün ifadeye katılmadığı anlaşılmıştır. Tüm gruplarda diğer katılımcılar bu ifade hakkında kararsız olduklarını belirtmişlerdir. Katılımcıların %48.4'ü kimlik avı gönderisi aldığını, %51.6'sı ise almadığını belirtmiştir. Siber saldırılar nedeniyle çevrim içi hizmetlere erişemeyen katılımcılar örneklemin %45.2'sini, bu durumu yaşamayan katılımcılar ise %54.8'ini oluşturmaktadırlar. Son olarak katılımcılara siber suç mağduru olmaları durumunda yetkililere bildirmeyi tercih edip etmeyecekleri sorulduğunda katılımcıların %87.1'i bildireceğini, %12.9'u ise bildirmeyeceğini belirtmiştir. Tablo 2'ye göre değişkenlerin tamamının ki-kare testi sonucunda anlamlı olduğu ($p < 0.05$) anlaşılmış ve $H_5, H_6, H_7, H_8, H_9, H_{10}, H_{11}, H_{12}, H_{13}, H_{14}$ ve H_{15} hipotezleri bu bulgular sonucunda kabul edilerek hipotezlerdeki ifadelerin sıralı lojistik regresyon analizine dahil edilmelerine karar verilmiştir.

Bulgular

Çoklu Doğrusal Bağlantı Testi

Sıralı lojistik regresyon analizi uygulanan değişkenler arasında çoklu doğrusal bağlantı sorununun olup olmadığını tespit etmek için çoklu doğrusal bağlantı testi gerçekleştirilmiştir. Çoklu doğrusal bağlantı testinden elde edilen varyans artış faktörü (VIF) değerlerinin 5 ile 10 arasında olması bağımsız değişkenler arasında orta düzeyde doğrusal bağlantı probleminin, 10'dan yüksek olması ise yüksek düzeyde çoklu doğrusal bağlantı probleminin olduğunu gösterir (Alkan ve Abar, 2020). Tablo 3 ve Tablo 4'te görülebileceği üzere tüm değişkenlerin VIF değerleri 5'ten küçük olup (1.05 ile 1.24 arasında) değişkenler arasında herhangi bir çoklu doğrusal bağlantı problemi söz konusu değildir.

Paralel Eğriler Varsayım Testi

Paralel eğriler varsayımı sıralı lojistik regresyon analizinin temel varsayımlarındandır. Bu varsayıma göre, lojistik regresyon analizinden elde edilen katsayıların kategorilere göre değişmemesi gerekir. Diğer bir deyişle, bağımlı değişken ile bağımsız değişkenler arasındaki ilişkiler, bağımlı değişkenlerin kategorilerinin hepsinde aynı şekilde gözlenmelidir. Bu varsayımın sağlanmadığı durumlarda sıralı lojistik regresyon modeli yerine multinomial regresyon modeli kullanmak gerekebilir (Kalfa ve Çakır, 2020).

Paralel eğriler varsayımının sağlanıp sağlanmadığını anlayabilmek için olabilirlik oran testi (likelihood ratio) veya Wald testi kullanılabilir (Akkuş ve Özkoç, 2016: 145). Bu çalışmada paralel eğriler varsayımının sağlanıp sağlanmadığını anlamak üzere olabilirlik oran testi gerçekleştirilmiştir. Buna göre 41 serbestlik derecesinde ki-kare değeri 181.33 olarak elde edilmiş ve katsayının %5 anlamlılık düzeyinde istatistiksel olarak anlamlı olduğu anlaşılmıştır ($p < 0.000$). Buna göre ilgili verinin modellenmesinde sıralı lojistik regresyon modelinin kullanılmasında bir sakınca yoktur.

Model Sonuçları

Bu çalışmada, bireylerin kendi internet ve dijital cihaz kullanım beceri düzeyleri hakkındaki düşüncelerini etkileyen faktörleri belirlemek üzere sıralı lojistik regresyon analizi uygulanmıştır. Lojistik regresyon analizinin öncesinde değişkenleri belirlemek ve hipotezleri test etmek amacıyla ki-kare analizi uygulanmıştır. Tablo 1’de sunulan Pearson ki-kare analiz sonuçlarına göre çalışmanın hipotezlerinden olan H1 hipotezinin sağlandığı görülmektedir. Buna göre yaş, cinsiyet, eğitim seviyesi ve istihdam durumu ile İDCK beceri düzeyleri arasında anlamlı bir ilişki bulunmaktadır ($p < 0.05$). Ayrıca Tablo 2’de sunulan Pearson Ki-kare analiz sonuçlarına göre çalışmanın hipotezlerinden olan H2 ve H3 hipotezlerinin sağlandığı görülmektedir. Buna göre siber güvenlik faaliyetleri ve siber suç bilinci ile İDCK beceri düzeyleri arasında anlamlı bir ilişki bulunmaktadır ($p < 0.05$).

Sıralı lojistik regresyon analizinin ardından uygulanan marjinal etki analizinden elde edilen marjinal etkiler Tablo 3 ve Tablo 4’te görüldüğü gibidir. Analizler sonucunda modelin istatistiksel açıdan anlamlı olduğu sonucuna ulaşılmıştır ($p < 0.000$). Sıralı lojistik regresyon analizlerinde modellerin uyum iyiliğini belirlemek için en sık kullanılan ölçütlerden biri McKelvey ve Zavoina (1975) tarafından geliştirilen McKelvey ve Zavoina R2 ölçütüdür (Selim, Selim ve Eroğlu, 2011). Bu çalışmada da modelin uyum iyiliği için McKelvey ve Zavoina’nın R2 ölçütü kullanılmış ve bu ölçütün değeri 0.711 olarak belirlenmiştir. Buna göre modelin uyum iyiliğinin kabul edilebilir olduğu anlaşılmıştır. Katılımcıların demografik özelliklerinin İDCK beceri düzeyi olasılıkları üzerindeki marjinal etkileri Tablo 3’te aktarılmıştır.

Tablo 3’e göre, erkeklerin kadınlara göre beceri düzeyinin başlangıç olma olasılığı %11 daha az iken uzman olması olasılığı %9.6 daha fazladır. Katılımcılardan 18-29 yaş aralığında olanlara göre 30-39 yaş aralığında olanların başlangıç düzeyde olma olasılığı %8.3 daha fazla iken uzman düzeyde olma olasılığı %7.2 daha az; 50 ve üzeri yaş grubunda olanların ise başlangıç düzeyde olma olasılığı %14.6 daha az iken uzman düzeyde olma olasılığı %12.7 daha fazla bulunmuştur.

Eğitim durumu ilk-orta-lise olanlara göre ön lisans mezunlarının beceri düzeyinin başlangıç olmasının olasılığı %19.8 daha az iken uzman olmasının olasılığı %17.2 daha fazla; lisans mezunlarının beceri düzeyinin ise başlangıç olmasının olasılığı %16.2 daha az iken, uzman olmasının olasılığı %14.1 daha fazladır. Katılımcılardan kamu sektöründe çalışanlara göre özel sektörde çalışanların beceri düzeylerinin başlangıç olması olasılığı %13.8 daha az iken uzman olması olasılığı %12 daha fazladır.



Tablo 3. Katılımcıların demografik özelliklerinin internet-dijital cihaz kullanım beceri düzeylerine göre marjinal etkileri

Değişken	dy/dx	Standart Hata	P>z	VIF
Cinsiyet: Erkek (Referans: Kadın)				1.14
Başlangıç	-0.11090	0.02812	0.000 ^a	
Orta	0.01441	0.00998	0.149 ^x	
Uzman	0.09649	0.02441	0.000 ^a	
Yaş: 30-39 (Referans: 18-29)				1.21
Başlangıç	0.08377	0.04619	0.070 ^c	
Orta	-0.01088	0.00908	0.231 ^x	
Uzman	-0.07288	0.04039	0.071 ^c	
Yaş: 50 ve üzeri (Referans: 18-29)				1.08
Başlangıç	-0.14624	0.08343	0.080 ^c	
Orta	0.01900	0.01673	0.256 ^x	
Uzman	0.12723	0.07199	0.077 ^c	
Eğitim: Ön lisans (Referans: İlk-Orta-Lise)				1.37
Başlangıç	-0.19809	0.05254	0.000 ^a	
Orta	0.02574	0.01699	0.130 ^x	
Uzman	0.17234	0.04798	0.000 ^a	
Eğitim: Lisans (Referans: İlk-Orta-Lise)				1.45
Başlangıç	-0.16265	0.03928	0.000 ^a	
Orta	0.02113	0.01344	0.116 ^x	
Uzman	0.14151	0.03700	0.000 ^a	
İstihdam: Özel Sektör (Referans: Kamu Çalışanı)				1.71
Başlangıç	-0.13885	0.05233	0.008 ^b	
Orta	0.01804	0.01342	0.179 ^x	
Uzman	0.12081	0.04558	0.008 ^b	

^a: p<0.000. ^b: p<0.05. ^c: p<0.10. ^x: p>0.10

Tablo 4'te katılımcıların İDCK beceri düzeylerini etkileyen değişkenlerin marjinal etkilerine yer verilmiştir. Tablo 4'e göre bilgisayarlarında Windows işletim sistemi kullanan katılımcılara göre kullandıkları işletim sistemini bilmeyenlerin beceri düzeylerinin başlangıç düzeyde olması olasılığı %22.9 daha fazla iken, uzman düzeyde olması olasılığı %19.9 daha azdır. Bilgisayar kullanmayan katılımcıların ise Windows işletim sistemi kullananlara göre beceri düzeylerinin başlangıç düzeyde olması olasılığı %20 daha fazla ve uzman düzeyde olması olasılığı %17.4 daha azdır.

Tablo 4. Katılımcıların internet-dijital cihaz kullanım beceri düzeylerini etkileyen değişkenlerin marjinal etkileri

Değişken	dy/dx	Standart Hata	P>z	VIF
Bilgisayar İşletim Sistemi: Bilmiyorum (Referans: Windows)				1.08
Başlangıç	0.22952	0.10023	0.022 ^b	
Orta	-0.02983	0.02213	0.178 ^x	
Uzman	-0.19969	0.08900	0.025 ^b	
Bilgisayar İşletim Sistemi: Kullanmıyorum (Referans: Windows)				1.17
Başlangıç	0.20081	0.04991	0.000 ^a	
Orta	-0.02609	0.01699	0.125 ^x	
Uzman	-0.17471	0.04602	0.000 ^a	
Mobil İşletim Sistemi: Bilmiyorum (Referans: Windows)				1.30
Başlangıç	0.33916	0.11780	0.004 ^b	
Orta	-0.04408	0.03094	0.154 ^x	
Uzman	-0.29508	0.10506	0.005 ^b	
Web sitesine girmeden önce yasallık kontrolü yaparım: Bazen (Referans: Asla)				1.54
Başlangıç	-0.07141	0.03964	0.072 ^c	
Orta	0.00928	0.00777	0.232 ^x	
Uzman	0.06213	0.03466	0.073 ^c	
Web sitesine girmeden önce yasallık kontrolü yaparım: Sıklıkla (Referans: Asla)				1.73
Başlangıç	-0.07446	0.04129	0.071 ^c	
Orta	0.00967	0.00823	0.240 ^x	
Uzman	0.06478	0.03589	0.071 ^c	
Bir e-posta veya gönderideki bağlantıya tıklamadan kontrol ederim: Bazen (Referans: Asla)				1.90
Başlangıç	-0.10619	0.06069	0.080 ^c	
Orta	0.01380	0.01161	0.235 ^x	
Uzman	0.09239	0.05318	0.082 ^c	
Geçen yıla kıyasla siber mağdur olma riski artmıştır: Katılıyorum (Referans: Katılmıyorum)				2.57
Başlangıç	-0.20215	0.09102	0.026 ^b	
Orta	0.02627	0.02000	0.189 ^x	
Uzman	0.17588	0.08025	0.028 ^b	
İnternette güvenliğimin artacağını bilirsem devletin gözetimini artırmasını kabul edebilirim: Kararsızım (Referans: Asla)				1.38
Başlangıç	0.07566	0.03960	0.056 ^c	
Orta	-0.00983	0.00827	0.235 ^x	
Uzman	-0.06582	0.03425	0.055 ^c	
İnternette güvenliğimin artacağını bilirsem devletin gözetimini artırmasını kabul edebilirim: Katılıyorum (Referans: Asla)				1.42
Başlangıç	0.08484	0.03447	0.014 ^b	
Orta	-0.01102	0.00857	0.199 ^x	
Uzman	-0.07381	0.02963	0.013 ^b	

a: p<0.000. b: p<0.05. c: p<0.10. x: p>0.10

Kullanıcıların mobil işletim sistemi kullanımına göre beceri düzeyleri değerlendirildiğinde Windows kullanan katılımcılara göre kullandıkları mobil işletim sistemlerini bilmeyen katılımcıların beceri düzeylerinin başlangıç düzeyde olması olasılığı %33.9 daha fazla iken uzman olması olasılığı %29.5 daha azdır. .



Bir web sitesine girmeden önce yasallığını bazen kontrol eden katılımcıların, bu kontrolü asla gerçekleştirmediğini belirten katılımcılara göre beceri düzeylerinin başlangıç olması olasılığı %7.1 daha az iken, uzman olması olasılığı %6.2 daha fazladır. Benzer şekilde sıklıkla web sitelerinde yasallık kontrolü yapan katılımcıların ise başlangıç beceri düzeyinde olmalarının olasılığı %7.4 daha az ve uzman beceri düzeyinde olmalarının olasılığı %6.4 daha fazladır.

E-posta ve gönderilerdeki bağlantılara tıklamadan önce kontrol edenlerin asla kontrol etmeyenlere göre, bu kontrolü bazen gerçekleştirenlerin beceri düzeyinin başlangıç düzeyde olması olasılığı %10.6 daha az iken, uzman düzeyde olması olasılığı %9.2 daha fazladır. Katılımcılardan geçen yıla kıyasla siber suç mağduru olma riskinin daha fazla olduğunu düşünenlerin düşünmeyenlere göre bu görüşe katılanların beceri düzeyinin başlangıç düzeyde olması olasılığı %20 daha az iken, uzman düzeyde olması olasılığı %17.5 daha fazladır. İnternette güvenliğin artması koşuluyla devlet gözetiminin artmasını kabul edebilirim görüşüne kararsız durumda olanların asla katılmıyorum diyenlere göre beceri düzeylerinin başlangıç düzeyde olması olasılığı %7.5 daha fazla ve uzman düzey olması olasılığı %6.5 daha az iken, devlet gözetiminin artmasını isteyenlerin beceri düzeylerinin başlangıç düzeyde olması olasılığı %8.4 daha fazla ve uzman düzeyde olması olasılığı %7.3 daha azdır.

Sıralı lojistik regresyon analizi sonuçlarına göre, katılımcıların cihazların güvenliği hakkındaki düşünceleri, şifrelerinin kişisel bilgi içerip içermemesi, tıklanan reklamlardaki tehlikeler hakkındaki farkındalık, önemli hesapların şifrelerinin değiştirilme sıklığı, kullandıkları yazılımları güncelleme davranışları, internet koruması kullanma durumu, siber suç tehlikesi ile ilgili bilgilendirilmiş hissetme durumu, kimlik avı gönderisi almış olma durumu, siber saldırı nedeniyle çevrimiçi hizmetlere erişememiş olma durumu ve siber suç mağduriyeti durumunda bildirme tercihi ile ilgili değişkenlerin katılımcıların internet ve dijital cihaz kullanım beceri düzeyi olasılıkları üzerinde istatistiksel açıdan anlamlı bir etki yaratmamaktadır.

Tartışma

Çalışma kapsamında sıralı lojistik regresyon analizi sonucunda elde edilen bulgular değerlendirildiğinde, demografik değişkenlere göre; 50 yaş ve üzerinde olanların, ön lisans ve lisans mezunlarının, erkeklerin ve özel sektör çalışanlarının dijital cihaz ve internet kullanım becerisi açısından kendilerini diğer insanlardan daha becerili görme eğiliminde olduğu belirlenmiştir.

Dijital bölünmede yaşın önemli faktörlerden biri olduğu bilinmektedir. Çünkü yaşlı bireylerin bilgi ve iletişim teknolojileri kullanmada engeller meydana gelebilmektedir. Görme, duyma problemleri gibi engellerin yanı sıra yaşlı bireylerin bilgi teknolojilerini kullanırken yaşadıkları zorluklar onları bu teknolojileri kullanmaktan uzaklaştırmakta, bu konudaki yeteneklerinin azalmasına yol açmaktadır (Baran vd., 2017). Ancak analiz sonuçlarında yaşlı bireylerin bu konuda gençlerden daha özgüvenli olduğu ortaya çıkmıştır. Buna dayanarak yaşlı bireylerin internet ve dijital kaynakları kullanım alışkanlıklarının incelenmesi ve eksik veya yanlış bildikleri noktaların düzeltilmesi açısından eğitimler sunulmasının yerinde olacağı düşünülmektedir.

Analiz sonuçlarına göre ön lisans ve lisans mezunlarının ilkokul, ortaokul ve lise mezunlarına göre daha yetkin olduklarını düşündükleri ortaya çıkmıştır. Eğitim düzeyi arttıkça dijital okuryazarlık yeteneğinin artacağı bilinmektedir (Bayrakçı, 2020). Dijital okuryazarlığı yüksek olan bireylerin internet ve dijital cihaz kullanımında yetkin oldukları düşünülmektedir. Bu açıdan ilkokul, ortaokul ve lise mezunu katılımcıların BİT erişimi ve kullanımı için çalışmalar yapılması önerilmektedir. Katılımcıların çalıştıkları sektörler incelendiğinde özel sektör çalışanlarının kamu çalışanlarına göre beceri düzeyi bakımından daha becerili olduklarını düşündükleri görülmüştür.

Katılımcıların internet ve dijital cihaz kullanım becerilerini etkileyen diğer değişkenlere incelendiğinde; kullandıkları bilgisayar ve mobil işletim sistemini bilmeyenlerin, bilgisayar kullanmayanların, web sitesine girmeden önce yasallık kontrolü yapmayanların, güvenliğin artması koşuluyla devlet gözetiminin artması konusunda kararsız olanların internet ve dijital cihaz kullanımı konusunda kendilerini diğerlerinden daha az yetenekli gördükleri belirlenmiştir. Ancak epostalarındaki bağlantıya tıklamadan önce kontrol etmeyen, geçen yıla kıyasla siber mağduriyet riskinin artmadığını düşünen ve internetteki güvenliği artması koşuluyla devlet gözetimini kabul eden katılımcıların kendilerini internet ve dijital cihaz kullanımı konusunda diğerlerinden daha yetenekli gördükleri anlaşılmıştır. Bu sonuçlardan hareketle benzer niteliklere sahip olan katılımcılara yönelik olarak günlük ve iş hayatında internet ve dijital cihaz kullanımı, siber güvenlik faaliyeti ve siber suç bilinci hakkında eğitimler düzenlenmesi faydalı olacaktır.

Sonuç ve Öneriler

Bu araştırmada, Osmaniye'deki 18 yaş ve üzeri bireylerin siber güvenlik faaliyetleri ve siber suç bilinci faktörleri ile internet ve dijital cihaz kullanım beceri düzeyleri arasındaki ilişkinin belirlenmesi amaçlanmıştır. Bu doğrultuda bireylerden elde edilen anket verilerine χ^2 bağımsızlık testi uygulayarak İDCK beceri düzeyleri ile bireylerin demografik özellikleri ile siber güvenlik faaliyetleri ve siber suç bilinci faktörleri arasında anlamlı ilişkiye sahip olmayan değişkenler belirlenip analiz kapsamından çıkartılarak geriye kalan değişkenler arasından çoklu doğrusal bağlantı testiyle sıralı lojistik regresyon analizi öncesi değişkenler hazır hale getirilmiştir.

Bireylerin İDCK beceri düzeyleri incelendiğinde; katılımcıların %22,6'sının başlangıç, %59,6'sının orta ve %17,8'inin uzman düzeyde olduğu açıklanmıştır. Benzer şekilde sosyodemografik değişkenlerden cinsiyet değişkeni incelendiğinde erkeklerin kadınlara kıyasla İDCK beceri düzeylerinin uzman kategorisi açısından daha yüksek olduğu ortaya çıkmıştır. Bununla birlikte yaş değişkeni değerlendirildiğinde, 18-29 yaş grubu arasında olanların yaş düzeyleri arttıkça diğer gruptakilere göre İDCK beceri düzeylerinin daha iyi olduğu anlaşılmıştır. Bununla birlikte bireylerin eğitim seviyesi arttıkça, İDCK beceri düzeylerinin arttığı belirlenmiştir.

Çalışma kapsamında sıralı lojistik regresyon analizi sonucunda elde edilen bulgular, siber güvenlik faaliyeti ve siber suç bilincine sahip olan bireylerin internet ve dijital cihaz kullanım beceri düzeylerinin daha yüksek düzeyde olduğunu ortaya koymaktadır.



İDCK beceri düzeyine sahip olan bireyler, dijital platformları daha etkin ve verimli bir biçimde kullanırken, bu platformlarda karşılaşılabileceği tehditleri bilerek bunlara karşı önlemler alarak bilgiye ulaşmakta, sosyal ve çalışma yaşamlarında daha başarılı olmaktadır. Başka bir ifadeyle, İDCK beceri düzeyleri bireylerin teknolojiyi etkin kullanarak bunları nasıl ve ne zaman kullanacağını bildikleri ve dijital hayatta aktif bir şekilde rol almalarını sağladığı için bu beceri düzeyleri çalışma hayatında önem arz etmektedir.

Günümüzün bilgi toplumu açısından her bir bireyin internet ve dijital cihaz kullanım becerilerinin kazandırılması, vatandaşlık hakkı olarak görülmeli ve bu temel teknoloji, araç ve becerilere ulaşması sağlanmalıdır. Bu doğrultuda toplum olarak eğitimde, sağlıkta, ekonomik ve kültürel alanlarda iyileştirmelerin sağlanabilmesi için kamu ve sivil toplum kuruluşlarının ortak çalışmalar yapması beklenmektedir.

Gelecekte yapılacak olan çalışmalarda kamu ve özel sektör çalışanlarının internet ve dijital cihaz kullanım becerilerinin karşılaştırmalı incelenmesi, bu çalışmada belirtilen grupların eğitime tabi tutulup eğitim öncesi ve sonrası düşüncelerinin ve becerilerinin karşılaştırmalı olarak incelenmesinin faydalı olacağı önerilmektedir.

Yazar Katkıları

Çalışmaya 1. Yazar: %50, 2. Yazar: %50 oranında katkı sağlamıştır.

Çıkar Çatışması

"Bireylerin İnternet-Dijital Cihaz Kullanım Becerilerini Değerlendirmelerinde Etkili Olan Faktörlerin Belirlenmesi" başlıklı makalemiz ile ilgili herhangi bir kurum, kuruluş, kişi ile mali çıkar çatışması yoktur ve yazarlar arasında da herhangi bir çıkar çatışması bulunmamaktadır.

Kaynakça

- Ağaoğlu, E. (2020). *İkinci Seviye Dijital Bölünme: Bireylerin Çevrimiçi Becerilerindeki Farklılıklar içinde (25-47)* Mehmet Fiğan ve Yeliz Dede Özdemir (Ed.) Dijital Kültür, Dijital Eşitsizlikler ve Yaşlanma. Alternatif Bilişim Derneği, Ankara.
- Akçakanat, Ö., Özdemir, O., & Mazak, M. (2021). İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi. *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5(2), 246-270.
- Akkuş, Ö., & Özkoç, H. (2016). *Stata Uygulamaları ile Nitel Veri Analizi Tercih Modelleri – Lojit Modeller – Probit Modeller*. Ankara: Seçkin | Sosyal Bilimler.
- Aksoy, B., & Erilli, N. A. (2021). Siber Suçların Siber Saldırılarına Maruz Kalan Şirketlerin Hisse Senedi Fiyatları Üzerindeki Etkileri. *İşletme Bilimi Dergisi*, 9(2), 237-259.

- Aksoy, N. C., Karabay, E., & Aksoy, E. (2021). Sınıf öğretmenlerinin dijital okuryazarlık düzeylerinin incelenmesi. *Selçuk İletişim*, 14(2), 859-894.
- Alkan. Ö., & Abar. H. (2020). Determination of factors influencing tobacco consumption in Turkey using categorical data analyses. *Archives of environmental & occupational health*. 75(1). 27-35. DOI: <https://doi.org/10.1080/19338244.2018.1556200>
- Alpar, R. (2013). Çok Değişkenli İstatistiksel Yöntemler, Detay Yayıncılık. Baskı, Ankara.
- Altınöz, M., Tosun, N., Çinkılıç, T., & Çay, E. (2019). Siber Güvenlik Ve Bilinçli Sosyal Medya Kullanımı Dersi Pilot Uygulamasına İlişkin Öğretmen Görüşleri. *Journal of Continuous Vocational Education and Training*, 2(1), 1-15.
- Álvarez Álvarez, M. D. C., & García-Prieto, F. J. (2021). Brecha digital y nuevas formas académicas en la escuela rural española durante el confinamiento. *Educar*, 57(2), 397-411.
- Alzubaidi. A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*. 7(1). e06016.
- Arıcak, O. T., Tanrıku, T., & Kınay, H. (2012). Siber mağduriyet ölçeği'nin ilk psikometrik bulguları. *Akdeniz Eğitim Araştırmaları Dergisi*, 11, 1-6.
- Atakan, M. (2021). Siber Güvenlik ve Covid 19 Salgının Uzaktan Denetim Üzerinde Etkileri . *Denetim*, 11 (22) , 27-39 .
- Bahar, A. (2018). Bilişim Suçları, İletişim Ve Sosyal Medya. *İstanbul Aydın Üniversitesi Dergisi*, 10(3), 1-36.
- Baran, A. G., Kurt, Ş. K., & Tekeli, E. S. (2017). Yaşlıların Dijital Teknolojileri Kullanım Düzeyleri Üzerine Bir Araştırma. *İletişim Kuram ve Araştırma Dergisi*, 45, 1-24.
- Baran, A. G., Kurt, Ş. K., & Tekeli, E. S. (2017). Yaşlıların Dijital Teknolojileri Kullanım Düzeyleri Üzerine Bir Araştırma. *İletişim Kuram ve Araştırma Dergisi*, 1(45).
- Blank, G., & Grosej, D. (2014). Dimensions of Internet use: amount, variety, and types. *Information, Communication & Society*, 17(4), 417-435.
- Bozkanat, E., & Başol, O. (2021). Dijital Becerilerin Cinsiyet Eşitliği İndeksine Etkisi: Ab Ülkeleri Üzerine Bir İnceleme. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 23(2), 587-603.
- Çakır, H., & Uzun, S. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 7(2), 353-379.
- Çapar, F., & Vural, Ö. F. (2013). Obstacle to e-government: Digital division E-devletleşme önündeki engel: Dijital eşitsizlik. *Journal of Human Sciences*, 10(1), 1674-1692.



- Çiftçi, A., Öksüz, M., Yolgeçen, Z., Akkuş B. & Alper, C. K. (2021). Üniversite Öğrencilerinin Siber Zorbalık ve Siber Mağduriyet Durumlarının Değerlendirilmesi. *Sosyal Hizmet*, 2021/2, 107-135.
- Dağlı, İ. (2022). Türkiye’de Bölgesel Düzeyde Dijital Bölünme: EDAS ve MAIRCA Yöntemleri ile Ampirik Bir Çalışma. *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 24(42), 359-386.
- Demir, N. & Büyükalın Filiz, S. (2018). Kamu Çalışanlarının Bilgi ve İletişim Teknolojilerini Kullanım Düzeylerinin İncelenmesi Sayıştay Başkanlığı Örneği. *Sayıştay Dergisi*, (108) ,149-174.
- Deniz, D., & Iriz, M. (2020). Covid-19 Pandemi Sürecinde Öğretmenlerde Siber Zorbalık Algısının Çeşitli Değişkenler ile İncelenmesi. Mehmet Necati Cizrelioğulları ve Rukiye Kılılı (Ed.), *ECLSS International Online Conference Economics & Social Sciences September 8-9 2020 Kyrenia Proceeding Book* içinde (s. 220). ECLSS International Online Conference Economics & Social Sciences September 8-9 2020 Kyrenia’da sunulan bildiri, Kyrenia.
- Eken, Ö., Tosun, N., & Eken, D. T. (2020). Covid-19 Salgını ile Acil ve Zorunlu Uzaktan Eğitime Geçiş: Genel Bir Değerlendirme. *Milli Eğitim Dergisi*, 49(1), 113-128. doi: 10.37669/milliegitim.780722
- Elena-Bucea, A., Cruz-Jesus, F., Oliveira, T., & Coelho, P. S. (2021). Assessing the role of age, education, gender and income on the digital divide: evidence for the European Union. *Information Systems Frontiers*, 23(4), 1007-1021.
- Erdoğan, E. (2021). Dijital Okuryazarlık ve Siber Zorbalık: Ortaokul Öğrencilerine Yönelik Bir İlişkisel Tarama Araştırması. *International Journal of Field Education*, 7(2), 61-76. Doi:10.32570/ijofe.1013788
- Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Personal Cyber Security Provision Scale development study Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *Journal of Human Sciences*, 12(2), 75-91.
- Erten, P. (2019). Dijital Bölünme. *Uluslararası Eğitim Bilim ve Teknoloji Dergisi*, 5(1), 15-23.
- Erten, P. (2019). Dijital bölünme. *Uluslararası Eğitim Bilim ve Teknoloji Dergisi*, 5(1), 15-23.
- EUROSTAT.(2020).
https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_sk_dskl_i&lang=en
- Gözler, A., & Taşçı, U. (2015). Sınıf Öğretmenliği Bölüm Öğrencilerinin Bilişim Suçları. *Bilişim Teknolojileri Dergisi*, 8(3), 147.
- Güner, O. (2022). Avrupa Birliği’nde Dijital Medya Okuryazarlığına Dair Bir Değerlendirme. *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (29), 473-499.

- Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1), 28-40.
- Ismailova, R., & Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. *Information Security Journal: A Global Perspective*, 25(1-3), 32-38.
- İlhan, Ü. D. (2021). A rapid implementation of remote work as a strategy in response to COVID-19: an examination in terms of work-life balance in (335-347) Hasan Dinçer & Serhat Yüksel (Ed.) *Management Strategies to Survive in a Competitive Environment*. Cham, Springer.
- Kalaycı, C. (2013). Dijital bölünme, dijital yoksulluk ve uluslararası ticaret. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 27(3), 145-162.
- Kalaycı, Ş. (2010). *SPSS uygulamalı çok değişkenli istatistik teknikleri*. Ankara, Turkey: Asil Yayın Dağıtım.
- Kalfa, V. R., & Çakır, E. (2020). Öğrencilerin Okudukları Bölümlerinden Duydukları Memnuniyeti Etkileyen Faktörlerin Sıralı Lojistik Regresyon Analizi ile Belirlenmesi. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, 8(5), 1413-1424.
- Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094.
- Karagiannopoulos, V., Kirby, A., Ms, S. O. M., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, 43, 105615.
- Karaođlan-Yılmaz, F. G., & Çavuş-Ezin, Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 7(2), 41-57.
- Kerman, B., Sönmez, A., & Kiraz, E. D. E. (2021). Halk Sağlığı Bakış Açısı ile Dijital Bölünme. *Climate and Health Journal*, 1(2), 58-67.
- Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme. *Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.
- Kılıç, S. (2013). Örneklem Yöntemleri. *Journal of Mood Disorders*, 3(1), 44-46. Doi: 10.5455/jmood.20130325011730
- Kiraz, O. Z. (2021). Siber Güvenlik Bağlamında Yeni Tehdit Algulamalarının Türkiye'nin Güvenlik Politikalarına Etkileri. *Journal of Management Theory and Practices Research*, 2(2), 69-88
- Kozan, M. & Bulut Özek, M. (2019). Böte Bölümü Öğretmen Adaylarının Dijital Okuryazarlık Düzeyleri Ve Siber Zorbalığa İlişkin Duyarlılıklarının İncelenmesi . Fırat Üniversitesi Sosyal Bilimler Dergisi , 29 (1) , 107-120 . DOI: 10.18069/firatsbed.538657



- Kuh, Z., & Erdem, R. (2022). Dijital Bölünmenin Sağlık Hizmetleri Kullanımı Üzerine Etkisi. *Mesleki ve Sosyal Bilimler Dergisi*, 3(1), 55-67.
- Kuvancı, B., & Akın, F. (2020). Dördüncü Sanayi Devriminin Bir Sonucu Olarak Siber Tehditler Ve Siber Güvenliğin Aile, Şirket Ve Devlet Bazında Önemi. *İş Ve Hayat*, 6(11), 24-45.
- Küçükvardar, M. (2018). Suç olgusunun değişen yüzü: Siber suçlar. *International Journal of Information, Technology and Philosophy*, 1(2), 1-18.
- McKelvey, R. D., & Zavoina, W. (1975). A statistical model for the analysis of ordinal level dependent variables. *Journal of mathematical sociology*, 4(1), 103-120. Doi: <https://doi.org/10.1080/0022250X.1975.9989847>
- Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, 43(2), 228-240. Doi: <https://doi.org/10.1080/01639625.2020.1806453>
- Mínguez, A. M. & Ballesteros, E. C. (2008). The Digital Divide in Education in the Knowledge Society in (430- 436) Goran D. Putnik & Maria Manuela Cunha (Ed.) *Encyclopedia of Networked And Virtual Organizations*, Hershey, PA; IGI Global.
- Nandal, S., Singla, J., & Rawal, S. (2021). The Waves of COVID 19 Era: A study on how it excavates the Digital Gap in Education System. *Elementary Education Online*, 20(5), 5367-5367.
- National Telecommunications and Information Administration (NTIA) (1995). Falling through the net: A Survey of the "Have nots" in rural and urban America. ERIC Clearinghouse. Retrieved 10.05.2022 from <http://www.ntia.doc.gov/ntiahome/fallingthru.html>
- National Telecommunications and Information Administration (NTIA)(1998). Falling Through the Net II: New Data on the Digital Divide. Retrieved 10.05.2022 from <http://www.ntia.doc.gov/ntiahome/net2/falling.html>
- National Telecommunications and Information Administration (NTIA) (1999). Falling through the net: Defining the digital divide. Retrieved 10.05.2022 from <http://www.ntia.doc.gov/ntiahome/fttn99/contents.html>
- Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber crime victimization among Internet active Nigerians: An analysis of socio-demographic correlates. *International Journal of Criminal Justice Sciences*, 8(2), 225.
- Nzeakor, O. F., Nwokeoma, B. N., & Ezech, P. J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology*, 14(1), 283-299.

- Nzeakor, O. F., Nwokeoma, B. N., & Ezech, P. J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology*, 14(1), 283-299.
- Öğün, M. N. & Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri*, 9, 18, 145-181.
- Özdoğan, A. Ç., & Berkant, H. G. (2020). Covid-19 pandemi dönemindeki uzaktan eğitime ilişkin paydaş görüşlerinin incelenmesi. *Milli Eğitim Dergisi*, 49(1), 13-43.
- Öztemiz, S., & Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası*, 14(1), 87-100.
- Öztürk, L. (2005). Türkiye'de dijital eşitsizlik: TÜBİTAK-BİLTEN anketleri üzerine bir değerlendirme. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 24(1), 111-131.
- Pagani, M. & Pasinetti, C. (2009). Accessibility, Usability, and Functionality in T-Government Services in (1-8) Margherita Pagani (Ed.) *Encyclopedia of Multimedia Technology and Networking (Second Edition)*, Hershey, PA; U.S.A, IGI Global.
- Pierce, J. (2019). *Digital Divide* in (1-8) *The International Encyclopedia of Media Literacy*. John Wiley & Sons.
- Qazi, A., Hasan, N., Abayomi-Alli, O., Hardaker, G., Scherer, R., Sarker, Y., ... & Maitama, J. Z. (2021). Gender differences in information and communication technology use & skills: a systematic review and meta-analysis. *Education and Information Technologies*, 1-34. doi: <https://doi.org/10.1007/s10639-021-10775-x>
- Sargedik, E. (2022). COVID-19 Pandemi Sürecinde Çocuklardaki İnternet Bağımlılığı, Siber Mağduriyet Düzeyleri ve Algılanan Ebeveyn İzleminin İncelenmesi. *Sağlık Bilimlerinde Değer*, 12(1), 65-72. DOI: <https://dx.doi.org/10.33631/sabd.1055300>
- Scheerder, A., Van Deursen, A., & Van Dijk, J. (2017). Determinants of Internet skills, uses and outcomes. A systematic review of the second-and third-level digital divide. *Telematics and informatics*, 34(8), 1607-1624.
- Seçkin-Kapucu, M. , Özcan, H. ve Karakaya-Özyer, K. (2021). The Relationship Between Middle School Students' Digital Literacy Levels, Social Media Usage Purposes and Cyberbullying Threat Level . *International Journal of Modern Education Studies*, 5 (2) , 537-566.
- Sekaran. U. (2003). *Research methods for business: A skill building approach (Fourth Edition)*. John Wiley & Sons Inc.
- Selim, H., Selim, S., & Eroğlu, S. (2011). Uluslararası Bir İmalat Firmasında Müşteri Memnuniyetini Belirleyen Faktörlerin Analizi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 26(3), 561-573.



- Serinikli, N. (2021). Covid-19 Salgın Sürecinde Örgütsel Değişim: Uzaktan/Evden Çalışma Modeli. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 31(1), 277-288.
- Seyran, F. (2021). Covid-19 ve Siber Zorbalık: Uzaktan Çalışma Üzerine Bir Değerlendirme. 2. Uluslararası Sosyal Bilimler ve İnovasyon Kongresi 24-25 Mayıs 2021, Ankara.
- Sezgin, S., & Fırat, M. (2020). Covid-19 pandemisinde uzaktan eğitime geçiş ve dijital uçurum tehlikesi. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 6(4), 37-54.
- Steinmetz, J. (2013). *Cyberbullying and The Digital Divide: Student and Teacher Perceptions and Reactions*. (Yayınlanmamış Doktora Tezi, The Ohio State University, Columbus).
- Şahin, A., Özkan, R. A., & Turan, B. N. (2022). İlkokul Öğrencilerine Yönelik Dijital Okuryazarlık Ölçeğinin Geliştirilmesi: Geçerlik ve Güvenirlik Çalışması. *Ana Dili Eğitimi Dergisi*, 10(3), 619-630.
- Talan, T., & Aktürk, C. (2021). Orta Öğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi*, 18(1), 158-180.
- Tekin, N. B. Ö., Süngü, B., Aydoğan, A. A., & Özer, D. (2022). Pandemi Sürecinde Araştırma Etiği Ve Dijital Bölünme Ekseninde Bir Çalışma Örneği: Engelli Bireyler Ve Annelerinin Yaşam Kaliteleri. *Sosyoloji Araştırmaları Dergisi*, 25(1), 88-100.
- Thomas, D. & Loader, B. (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge
- UNESCO. (2018). Digital skills critical for jobs and social inclusion.
- Uyar, M., & Hasdemir, T. (2021). Çocukların İnternet'e Erişimleri Ve Kullanım Becerileri: Ankara İli Örneği. *Ufuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 10(19), 7-38.
- Ünal, Y. (2009). Bilgi toplumunun tarihçesi. *Tarih Okulu Dergisi*, (5),123-144.
- Wang, D., Zhou, T., & Wang, M. (2021). Information and communication technology (ICT), digital divide and urbanization: Evidence from Chinese cities. *Technology in Society*, 64, 101516.
- Yakut, E. (2020). Multinomial Probit Model İle Konut Seçimine Etki Eden Faktörlerin Belirlenmesi: Osmaniye İli Uygulaması. *Business & Management Studies: An International Journal*, 8(3), 3274-3301.
- Yılmaz, A. (2021). Covid 19 Pandemi Sürecinde Evden Çalışma ve Koordinasyon Sorunları içinde (173-202) Ebru Ertürk (Ed.) Covid 19 Pandemi Sürecinde Çalışma Yaşamındaki Değişime Örgütsel Davranış Konuları Perspektifinden Bakış. Gazi Kitabevi, Ankara.
- Yontar, A. (2019). Öğretmen adaylarının dijital okuryazarlık düzeyleri. *Ana Dili Eğitimi Dergisi*, 7(4), 815-824.

Zayid, E. I. M., & Farah, N. A. A. (2017). A study on cybercrime awareness test in Saudi Arabia-Alnamas region. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 199-202). IEEE.

Extended Abstract

The concept of digital division, defined as inequality in access to information and communication technologies, has become a research subject that has gained depth as a result of a movement of change which has been led by technology (Sezgin and Firat, 2020; Capar and Vural, 2013; Unal, 2009). Certain groups may be disadvantaged depending on the content of the concept of digital division. For example, older individuals can be in disadvantageous situation with respect to younger individuals, as well as those with lower level of education compared to those with higher level of education and those with lower level of income compared to those with higher level of income (Ozturk, 2005); Agaoglu, 2020). However, with the effect of the Covid-19 pandemic, most of the business life, education life and daily activities started to be carried out over the internet and digital devices through remote access systems, and access and usage competencies in this regard have become a necessity without considering any disadvantages. (Bayrakci, 2020). Especially many individuals who were left incompetent in terms of Internet and digital device use as a result their business, educational, and daily life activities being carried over to the Internet have started to spend more time on the Internet than they usually did, and this situation has created larger gaps in terms of digital victimization (Sarigedik, 2022; Seyran, 2021; Deniz and Iriz, 2020). For this reason, it has become an important issue for individuals to have information about the use of the internet and digital devices for their security in the internet environment and to try to improve themselves in this respect. Competence for Internet and digital device use has been defined by UNESCO (2018) as the skill that one needs to have in order to use digital devices and Internet applications so as to access and manage information. In the present study, the factors that affected competence levels of individuals for using the Internet and digital devices were investigated.

Th study data were collected through a survey form which included questions regarding gender, age, educational status, and employment status, and some statements borrowed from the Cyber Security Activities and Cyber Crime Awareness sections of the Information Security Awareness Scale designed by Alzubaidi (2021). In addition, the level of Internet and digital device use (IDDU) variable, by which the individuals evaluated their own competence of Internet and digital device use, was determined as the dependent variable. With this variable, the individuals evaluated their competences over three levels (Beginner:1, Intermediate:2, Advanced:3). The population of the study consisted of individuals over the age of 18 years who lived in Osmaniye province. The study sample included 522 observed individuals, 118 of whom reported to be at the beginner level, 311 at the intermediate level, and 93 at the advanced level in terms of Internet and digital device use.

In order to determine the variables that could be included in the ordinal logistic regression analysis in the study, Pearson Chi-square analysis was performed. Accordingly, multiple linear test and



parallel lines assumption test were performed for the significant variables in the Chi-square analysis ($p < 0.05$). As a result, it was understood that the data were suitable for ordinal logistic regression analysis. Following the ordinal logistic regression analysis performed, marginal effects analysis was performed in order to calculate the effects of the factors on the probabilities of Internet and digital device use levels.

According to the results of the Pearson Chi-square analysis, the relationship of the individuals' demographic characteristics, cyber security activities, and cyber crime awareness with their Internet and digital device use levels was confirmed. The ordinal logistic regression analyses proved that the model was significant ($p < 0.000$). One of the criteria used most frequently in order to determine goodness of fit in ordinal logistic regression analyses is R^2 criterion developed by McKelvey and Zavoina (1975) (Selim, Selim and Eroglu, 2011). In the present study, McKelvey and Zavoina's R^2 criterion was used for the goodness of fit of the model, and the value of the criterion was determined as 0.711. Thus, it was understood that the model's goodness of fit was acceptable. Moreover, based on the results of the ordinal logistic regression analysis of demographic variables, it was determined that those aged 50 years and above, those who had bachelor's and associate degree, males, and private sector employees had a tendency to evaluate themselves more competent in terms of Internet and digital device use than other individuals.

According to the results of the marginal effects analysis, it was determined that those who did not know the operation system of the computer and mobile device they used, those who did not use a computer, those who did not run legality check before entering a website, those who were undecided about increased government supervision on the condition that security was enhanced considered themselves less competent in terms of Internet and digital device use compared to other individuals. However, it was also found that the participants who did not check before clicking the link in their e-mails, those who thought that cyber victimization risk did not increase more compared to the previous year, and those who accepted increased government supervision provided that security on the Internet was increased evaluated themselves more competent in terms of Internet and digital device use in comparison to other individuals. Based on these, it is believed that it will be beneficial to organize training programs aimed at individuals with similar characteristics on Internet and digital device use in daily and business life, cyber security activities, and cyber crime awareness.

Individuals who have a good level of competence for Internet and digital device use make use of digital platforms more efficiently and effectively, they have access to information by being aware of the threats they may encounter on these platforms and taking necessary precautions, and they become more successful in their social and business lives. From today's information society perspective, getting each individual to gain skills for Internet and digital device use should be seen as a citizenship right, and their access to these basic technologies, devices, and skills should be ensured. In this direction, governments and non-governmental organizations should make collaborative efforts in order to ensure improvements in education, health, and economic and cultural areas as a society.