MANAS Sosyal Araştırmalar Dergisi 2024 Cilt: 13 Sayı: 3
MANAS Journal of Social Studies 2024 Volume: 13 No: 3
ISSN: 1694-7215
Research Paper / Araştırma Makalesi

# Planlı Davranış Teorisi Kapsamında A/B Kişilik Tipine Göre Siber Güvenlik Farkındalığı: Üniversite Öğrencileri Üzerine Araştırma

Tuğçe ŞİMŞEK[1]

**Öz**

Bireyler arasındaki farklı kişilik tipleri, siber güvenlik farkındalığının etkin bir şekilde geliştirilmesi açısından önemli bir role sahiptir; çünkü bu tipler, kullanıcıların güvenlik konularına yönelik tutumları ve tepkileri üzerinde belirgin bir etki yapabilir. Siber güvenlik de dijitalleşmenin artması ve dijital çağa doğan nüfusun artması ile üzerinde durulması gereken bir gerçek olarak karşımıza çıkmaktadır. Hem özel hayatta hem de çalışma hayatında siber güvenlik farkındalığına sahip olmak kişilerin de kendilerini ve hatta kişisel bilgilerini güvende tutmalarını sağlamaktadır. Son dönemlerde örgütler tüm çalışanlarının siber güvenlik konusunda yeterince bilgiye sahip olmalarını istemektedir. Planlı Davranış Teorisi ışığında siber güvenlik farkındalığının iş hayatında yerini almaya başlayacak olan üniversite öğrencilerindeki durumunu analiz etmek literatüre katkı sağlayacaktır. Bunun yanı sıra çalışmanın sorunsalı A ya da B kişilik tipine sahip olan üniversite öğrencilerinin siber güvenlik farkındalığı konusunda bir farklılık gösterip göstermediğidir. Çalışmanın örneklemi bir devlet üniversitesinde okumakta olan üniversite öğrencilerinde kartopu örneklem yöntemi ile oluşturulmuştur. Verilerin analizinde SPSS Statistics 25 kullanılmıştır. Tanımlayıcı analiz ve iki bağımsız örneklem arasındaki farkın öneminin sınanması için Mann-Whitney Testi kullanılmıştır. 172 katılımcı üzerinden yapılan analiz neticesinde; A ve B kişilik tipine göre siber güvenlik farkındalığı istatistiksel olarak anlamlı bir farklılığa sahiptir. Buna ek olarak cinsiyete göre siber güvenlik farkındalığı da anlamlı bir farklılık göstermiştir. A tipi kişiliğe sahip katılımcıların siber güvenlik farkındalığı ortalaması 2,52 olarak tespit edilmiştir. B tipi kişilikteki katılımcıların ise siber güvenlik farkındalığı ortalaması 2,12 olarak bulunmuştur. Çalışmanın sonuçlarına göre katılımcılar arasında A kişilik tipine sahip ve kadın katılımcıların siber güvenlik farkındalığı daha yüksektir.

*Anahtar Kelimeler:* Planlı Davranış Teorisi, A/B Tipi Kişilik, Siber Güvenlik, Siber Güvenlik Farkındalığı

# Cyber Security Awareness According to A/B Personality Type within the Scope of Theory of Planned Behavior: A Study on University Students

**Abstract**

Different personality types among individuals play an important role in the effective development of cybersecurity awareness, as they can have a significant impact on users' attitudes and reactions to security issues. Cybersecurity is also a reality that needs to be addressed with the increase in digitalization and the growing population born into the digital age. Having cyber security awareness in both private and working life enables people to keep themselves and even their personal information safe. Recently, organizations want all their employees to have enough knowledge about cyber security. In the light of the Theory of Planned Behavior, analyzing the situation of cyber security awareness in university students who will start to take their place in business life will contribute to the literature. In addition, the problematic issue of the study is whether university students with personality type A or B show a difference in cyber security awareness. The sample of the study was formed by snowball sampling method among university students studying at a state university. SPSS Statistics 25 was used to analyze the data. Descriptive analysis and Mann-Whitney Test were used to test the significance of the difference between two independent samples. As a result of the analysis on 172 participants; cyber security awareness has a statistically significant difference according to personality types A and B. In addition, cyber security awareness also showed a significant difference according to gender. The average cyber security awareness of the participants with type A personality was found to be 2.52. The average cyber security awareness of the participants with type B personality was found to be 2.12. According to the results of the study, the cyber security awareness of the participants with personality type A and female participants is higher.

*Keywords:* Theory of Planned Behavior, Type A/B Personality, Cyber Security, Cyber Security Awareness

**Atıf İçin / Please Cite As:**

Şimşek, T. (2024). Planlı davranış teorisi kapsamında A/B kişilik tipine göre siber güvenlik farkındalığı: Üniversite öğrencileri üzerine araştırma. *Manas Sosyal Araştırmalar Dergisi, 13*(3), 1066-1074. doi:10.33206/mjss.1300491

**Geliş Tarihi / Received Date:** 22.05.2023 **Kabul Tarihi / Accepted Date:** 10.02.2024

[1] Dr. Öğr. Üyesi - Gümüşhane Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, tugce.simsek@gumushane.edu.tr,
ORCID: 0000-0003-3256-4348

## Giriş

Bir kişinin kişiliği hakkında konuşulduğunda, o kişiyi diğer insanlardan farklı, hatta belki de benzersiz kılan şeylerden bahsedilmektedir. Boeree (2017) kişilik teorilerini anlattığı kitabında kişiliğin bu yönünü bireysel farklılıklar olarak adlandırıldığını belirtmiştir. Kişilik kuramcıları insanlar arasındaki ortak noktalarla da ilgilenirler. Örneğin, nevrotik kişi ile sağlıklı kişinin ortak noktası nedir? Ya da insanlarda bazılarında içe dönüklük, bazılarında ise dışa dönüklük olarak kendini ifade eden ortak yapı nedir? Bunu söylemenin bir başka yolu da kişilik kuramcılarının bireyin yapısıyla, özellikle de psikolojik yapısıyla ilgilendikleridir. İnsanlar nasıl "bir araya gelirler"; nasıl "çalışırlar"; nasıl "dağılırlar". Bazı teorisyenler bir adım daha ileri giderek kişi olmanın özünü aradıklarını söylerler. Ya da bireysel bir insan olmanın ne anlama geldiğini aradıklarını söylerler. Kişilik psikolojisi alanı, insanlar arasındaki farklılıklar için oldukça basit bir ampirik araştırmadan, hayatın anlamı için oldukça felsefi bir araştırmaya kadar uzanmaktadır. Bu çalışma ise farklı kişilik tipine sahip bireylerin sergiledikleri davranışlardaki farkın üzerine vurgu yapmayı hedeflemektedir. Genel olarak günlük hayatın akışındaki iş ve özel yaşamda bireylerin davranışlarından yola çıkarak kişilik tipinin belirlenebildiğini görülmektedir. Bunun bir örneği de Rosenman ve Friedman'ın A ve B Tipi kişilik sınıflandırmasıdır. Çalışmada tercih edilen A ve B tipi kişilik sınıflandırması ile bu kişilerin siber güvenlik farkındalığının kişilik tiplerine göre değişiklik gösterip göstermediğinin tespit edilmesi çalışmanın amacını oluşturmaktadır. A ve B tipi kişilik sınıflandırması ile ilgili yapılan araştırmaların kişilik tiplerine göre davranışsal çıktılara olan etkiler üzerine yoğunlaştıkları fark edilmektedir. Son yıllarda dijitalleşmenin artması ile de bireylerin çalışma hayatlarında ve özel hayatlarında sürekli bilgisayar, akıllı telefon ve internet kullanımına maruz kaldıkları görülmektedir. Bu maruziyet doğrultusunda bireylerin siber güvenlik kavramını içselleştirmeleri gerekmektedir. Literatürde kişilik tiplerine bağlı olarak bireylerin tutum ve davranışlarındaki farklılıklar ile ilgili çalışmalar görülmektedir. Bu çalışma ise literatürde karşılaşılmayan bir durum olarak; kişilik tipinin planlı davranış teorisi (Ajzen, 1985) perspektifinde siber güvenlik farkındalığındaki farklılığı ele almıştır. Teknolojik gelişmeler ile birlikte kişilik tiplerinin bu gelişmelere ne derece adapte olabileceğini ortaya koyan öncül çalışmalardan birisi olma ve gelecek çalışmalar için yol gösterici nitelikte olma özelliği taşımaktadır. Planlı davranış teorisi kapsamında kişilik tipinin bir bireyin siber güvenlik farkındalığına üzerinde bir farklılık oluşturabileceği düşünülmektedir (van der Schyff ve Flowerday, 2021).

## Kavramsal Çerçeve

### Planlı Davranış Teorisi Kapsamında A/B Tipi Kişilik Tipleri

Kişilik tipleri (A/B) ekseninde siber güvenlik farkındalığının tartışıldığı çalışmanın dayanak noktası Planlı Davranış Teorisidir. Planlı Davranış Teorisi (PDT) Ajzen (1985) tarafından sosyal psikoloji teorisi olarak ortaya konulmuştur. Planlı Davranış Teorisi, Mantıklı Eylem Teorisinin genişletilmiş bir modelidir ve sosyal psikologlar için davranışsal niyeti tahmin etmek için en kapsamlı modellerden biridir (Ahmed, Li, Khan, vd., 2021). Planlı Davranış Teorisi, Nedensel Davranış Teorisinin aksine insan davranışının her zaman rasyonel olmadığı, davranışın faydalarını her zaman göz önünde bulundurmadığını ve tümünün bireyin kontrolünde olmadığını savunmaktadır. Planlı Davranış Teorisine göre bireylerin davranışlarının %20-30'luk kısmının niyetleri ile açıklanabildiği belirtilmiştir (Sönmez, 2022). PDT' ye göre birey davranışlarının ana unsuru niyettir. Davranışsal niyet, davranışın gerçekleştirilmesi için üç eğilime sahip olmalıdır. Bunlar: davranışa ilişkin tutumlar, sübjektif norm, algılanan davranış kontrolüdür. Yapılan bazı çalışmalar farkındalığın niyet üzerinde olan etkisini ortaya koymuştur (Başarır, 2020; İlter, 2020). Başka bir çalışmada ise Mathieson (1991) kullanıcıların bir bilgi sistemini kullanma niyetlerini tahmin etmek için teknoloji kabul modeli ile planlı davranış teorisini karşılaştırmıştır. Mathieson'ın çalışmasının sonucu, her iki modelin de kullanıcı niyetlerini iyi tahmin ettiğini ve teknoloji kabul modelinin uygulanması en kolay teori olmasına rağmen, Planlı Davranış Teorisinin daha spesifik bilgiler sağladığını göstermiştir. Harrison ve diğerleri (1997) küçük işletme yöneticilerinin bir bilgi teknolojisini benimseme kararlarını açıklamak ve tahmin etmek için Planlı Davranış Teorisi'ni kullanmıştır. Planlı Davranış Teorisi'nin yöneticilerin karar sürecini açıklamakta faydalı olduğunu, karar sürecinin benimsemeye yönelik tutum, benimsemeye yönelik öznel norm ve benimseme üzerinde algılanan kontrolün bir fonksiyonu olduğunu bulmuşlardır. Bu bağlamda; Planlı Davranış Teorisi kapsamında farkındalığın niyeti etkilemesi ile niyetin de davranışa olan etkisi görülmektedir. Buna göre Planlı Davranış Teorisinin savı dikkate alınarak; siber güvenlik farkındalığının siber güvenlik davranışına yönelme niyetini ortaya çıkaracağı ve bu niyetin siber güvenlik davranışını ortaya çıkaracağı düşülmektedir. Bu çalışma ise siber güvenlik farkındalığının tespit edilmesini hedeflemektedir. Farkındalığın tespiti ise niyet ve akabinde siber güvenlik davranışının ortaya çıkması konusunda öngörümleme fırsatı vermektedir. A ve B Tipi Kişiliğin siber güvenlik davranışı farkındalığının

ortaya konulmaya çalışıldığı bu çalışmada, kişilik tiplerine göre siber güvenlik farkındalığında bir farklılık olup olmadığı da araştırılmıştır.

### Rosenman ve Friedman A ve B Tipi Kişilik

Kişilik, bireyden kaynaklanan tutarlı davranış kalıpları ve içsel süreçler olarak tanımlanabilir (Burger, 2015). Türk Dil Kurumu güncel sözlük kişiliği "Bir kimseye özgü belirgin özellik, manevi ve ruhsal niteliklerinin bütünü, şahsiyet" olarak tanımlamıştır (TDK, 2022).

Rosenman ve Friedman'ın A Tipi davranışı belirlemek için kullandıkları ilk yöntem yapılandırılmış bir görüşme ve görüşmecileri eğitmek için kullanılan ses kasetleri olmuştur (Kittel, Kornitzer, & Dramaix, 1986). Görüşmecilerini kalp hastaları arasından seçen Rosenman ve Friedman A tipi kişilik davranışını ortaya atmıştır (Rosenman ve Friedman, 1961). Çalışmalarında hasta gruplarını A ve B olarak ayrımlamışlardır. B tipi kişilik davranışı sergileyen bireylerin ise A tipi kişilik davranışı sergileyen bireylerin ters kutbunda bir davranış sergiledikleri görülmektedir. Rosenman ve Friedman A grubu hastalarını seçerken aynı davranış sergileyen altı kadın yöneticiden belirli davranış örüntüsü sergileyen görünüşte sağlıklı klinik kalp rahatsızlığı olmayan kadınlara ulaşılmasını istemişlerdir. Açık davranış modeli A'nın yönleri ise şu şekilde belirtmişlerdir: (1) başarı, ilerleme ve tanınma için sürekli, agresif "dürtü", (2) rekabet gücü ve kazanma arzusu, (3) "son teslim tarihleri"nin zaman baskısına tabi olan birden çok mesleki ve meslek dışı katılıma alışılmış katılım, (4) olağanüstü zihinsel ve fiziksel uyanıklık ve (5) çoğu fiziksel ve zihinsel işlevi yerine getirme hızlarını artırmaya yönelik alışılmış eğilim. A davranış modelinin karşıtı olarak B davranış modelini sergileyen bireylerdeki özellikleri ise şu şekilde açıklamışlardır: sakinlik sergileyen kadınlar, ilerleme ve tanınma dürtüsünün görece yokluğu, saldırganlık, rekabet etme arzusu, hırslılık, mesleki son teslim tarihlerine katılım, zaman aciliyeti hissi veya konuşmayı hızlandırma eğilimi, zihinsel ve fiziksel işlevler. B grubunu oluşturan grup araştırmacılar tarafından karşıt davranış kalıpları temelinde meslekten olmayan seçiciler tarafından seçilen kişiler olarak tanımlanmaktadır. A ve B tipi kişiliğin temelleri bu çalışma ile ortaya konmuştur.

**Tablo 1:** *A tipi kişilik ve B tipi Kişilik karşılaştırması*

| A Tipi Kişilik | B Tipi Kişilik |
|---|---|
| Başarı için saldırgan davranış gösterir. | Rekabet etmeyi sevmezler. |
| Hırslı bir yapıya sahiptirler. | Hırslı bir yapıları yoktur, mükemmeliyetçi değillerdir. |
| Tüm işlerde hıza önem verirler, sabırsızdırlar. | İşlerini daha rahat ve düzenli yapmayı tercih ederler. |
| Benmerkezcilerdir. | İşbirlikçi bir yapıya sahiptirler. |
| Yeniliğe açıktırlar. | Nitelikli iş yapmak isterler. |
| Başkaları tarafından takdir edilme isteği vardır. | Çevrelerindeki insanları kendilerine daha az rakip görürler. |
| Kendilerine boş zaman ayırmak onlar için zordur. | Kendilerine zaman ayırırlar, sosyal ve iyi geçimli insanlardır. |
| Fiziksel aktivite yapmayı çok az uygular. | Fiziksel aktivite yapar. |

**Kaynak:** Tablo yazar tarafından oluşturulmuştur. Tablonun oluşturulmasında kullanılan kaynaklar: Bilgin Yurdaöz ve Cemaloğlu, (2021), Yıldız ve Özsoy, (2013), Koçak, Eti ve Gürsoy, (2017/2)

A Tipi ve B tipi Kişilik ile ilgili literatürde yerini almış bazı araştırmalara bakıldığında; Üzüm ve Şenol (2019) A ve B tipi kişiliğin presenteizme etki etmediği sonucunda ulaşmışlardır. Koçak, Eti ve Gürsoy (2017/2) A ve B tipi kişiliğe sahip kamu ve özel sektör çalışanlarının örgüt kültürünün gerektiği şekilde A tipi ve B tipi davranış sergilemediklerini ortaya koymuşlardır.

### Siber Güvenlik Farkındalığına İlişkin Literatür ve Hipotezler

Bilgi teknolojisinin gün geçtikçe geliştirilmesi internet kullanan kişi sayılarının artmasını beraberinde getirmiştir. İnternet kullanımı ise bireylerin bilgi güvenliğinin farkına varmaları gerekliliğini doğurmuştur. İnternet kullanımı ile güvenlik riskleri artmaktadır. Örneğin; şifreler, gizli veriler, bankacılık işlemleri, sosyal medya kullanımı vb. güvenlik riski oluşturan unsurlardır. Bireylerin siber saldırılara karşı siber güvenlik farkındalığına sahip olması ve bu farkındalığın artırılması önemli hale gelmiştir. Siber güvenlik farkındalık kampanyası kapsamında yapılmış bir çalışmada siber güvenlik farkındalığının artırılması, mesajın düzenli olarak pekiştirilmesi gerektiğinden ve her gün yeni internet kullanıcıları olduğundan devam eden bir görev olduğu belirtilmiştir (Chang ve Coppel, 2020). Siber güvenlik farkındalığını konu alan ve bilgisayar bilimleri ve medya bilimleri öğrencileri üzerine yapılan bir araştırmada ise her iki disiplinde öğrenim gören öğrencilerin siber güvenlik farkındalığı ve davranışına ilişkin öznel verilerin ortalama sıra farklarına dayanan sonuçlarında; bilgisayar bilimleri ve medya bilimleri öğrencilerinin sorunun önemli bir kısmına karşı aynı tutuma sahip olmalarına rağmen, siber güvenliğin baskın alanlarının bilgisayar bilimleri öğrencilerinin daha iyi performans gösterdiği alanlar olduğunu göstermiştir (Huraj, Lengyelfalusy, Anna Hurajová ve Lajčin, 2023).

Yakın tarihli siber güvenlik farkındalığını konu alan bazı araştırmalara bakıldığında hala bu farkındalığın tam oluşmadığı görülmektedir. Alzubaidi (2021) yılında yapmış olduğu çalışmasında; 1230 katılımcının %31,7'sinin internete erişmek için halka açık Wi-Fi kullandığını, %51'inin şifrelerini oluşturmak için kişisel bilgilerini kullandığını, %32,5'inin kimlik avı saldırıları hakkında herhangi bir fikri olmadığını, %21,7'sinin siber suç mağduru olduğunu ve sadece %29,2'sinin suçu bildirdiğini göstermiştir ki bu da farkındalık düzeylerini yansıtmaktadır. Trim ve Lee (2019)'nin çalışmasında ise B2B pazarlamacılarının, personelin siber saldırganların eylemlerine karşı koymasına yardımcı olmak için uygun bir siber güvenlik farkındalık programı tasarlarken ve uygularken koordinatör rolü oynayabileceği belirtmişlerdir. Öz yeterlilik ve algılanan beklenti arasındaki farkın azaltılmasıyla, personelin güven düzeyi artacak ve kurum genelinde tutumsal davranış değişikliği meydana gelecektir.

Tuğal, Almaz ve Sevi'nin (2021) çalışmasında siber saldırı yöntemlerini, siber zayıflıklar için çözümleri, kullanıcılara siber farkındalık eğitimlerinin verilmesinin gerekliliğini, bilgi sistemleri altyapılarının güçlendirilmesi gerektiğini, siber farkındalık eğitimlerindeki sürecin nasıl olması gerektiği konularına değindikleri görülmüştür. Tuğal vd. (2021) siber güvenlik farkındalığının eğitiminde üniversite personeli ve öğrencilerinin bu eğitime ulaşabilmesinde izlenmesi gereken bir hiyerarşinin eğitimin herkese ulaşmasını kolaylaştıracağını belirtmiştir.

Gündüzalp (2021) üniversite çalışanlarının siber güvenlik farkındalığını tespit ettiği çalışmasında özellikle bilgi işlem daire başkanlığı çalışanlarını dikkate almıştır. Çalışmasının sonucunda çalışanların siber güvenlik farkındalıklarını yüksek düzeyde tespit etmiştir.

Aksoğan, Bayer, Gülada ve Çelik (2018) İletişim Fakültesinde öğrenim gören öğrenciler üzerine yapmış oldukları çalışmalarında öğrencilerin büyük bir çoğunluğunun siber güvenlik farkındalığına sahip olmadıklarını ortaya koymuşlardır.

Yapılan literatür taramaları ışığında kişilik tiplerine bağlı olarak kişilerin sahip olduğu siber güvenlik farkındalığı arasında anlamlı bir farklılık olup olmadığı yönünde araştırmanın sonuçlandırılabilmesi adına Hipotez 1 ve Hipotez 2 kurulmuştur.

**$H_1$:** Siber güvenlik farkındalığı A/B Kişilik Tipine Göre anlamlı farklılık göstermektedir.

**$H_2$:** Siber güvenlik farkındalığı cinsiyete göre anlamlı farklılık göstermektedir.

## Yöntem

A ve B kişilik tiplerine göre siber güvenlik farkındalığının tespit edilmeye çalışıldığı bu çalışmada nicel araştırma yöntemi kullanılmıştır. Nicel araştırma deseni olarak ilişkisel tarama kullanılmıştır.

### Evren - Örneklem

Araştırma evreni bir devlet üniversitesinde okumakta olan öğrencileri kapsamaktadır. Bu öğrenciler arasından basit tesadüfi örneklem yöntemi ile katılımcılar temin edilmiştir. Yüz yüze anket yöntemi ile veriler (Ekim 2022- Ocak 2023 tarih aralığında) elde edilmiştir. Örnekleme ulaşılmasında kartopu örneklem yöntemi kullanılmıştır. Kartopu örnekleme yönteminin tercih edilmesindeki neden araştırmanın yapıldığı üniversitedeki bazı bölümlerin aktif öğrenci almamaları ve öğrencilerin fakülte binalarında sayılarının az olmasıdır. Toplamda 183 katılımcının verilerinin 172 tanesi SPSS programına işlenmiştir. 8 katılımcı çalışmanın ana ölçeği olan siber güvenlik farkındalığı sorusuna cevap vermemiştir. 3 katılımcı ise kişilik tiplerinin belirlenmesinde kullanılan ölçek maddelerinden bazılarını boş bırakmıştır. Bu eksiklerin çalışma sonucunu yanlış yönlendirmemesi adına soruları eksiksiz dolduran 172 katılımcının verileri dikkate alınmıştır.

### Veri Toplama Araçları

*Siber Güvenlik Farkındalığı Ölçeği.* Zwilling, Klien, Lesjak, Wiechetek, Cetin ve Basim' ın(2022) tek soru ile ölçümlemiş oldukları siber güvenlik farkındalığı ölçeği kullanılmıştır. Kullanılan ölçekte katılımcıların "Siber güvenlik terimine ne kadar aşinasınız?" sorusuna bilgisiz, az bilgili, bilgili ve çok bilgili olarak cevap vermeleri istenmiştir.

*A/B Tipi Kişilik Ölçeği.* Üçok' un (2006) Liderlik ve Yönetici- Davranış Geliştirme adlı kitabında yer alan Tip A- Tip B testi kullanılmıştır. Her kişilik tipi için 7 ifadenin değerlendirilmesi istenmiştir. Bu değerlendirme 1-8 arası bir numaralandırma ile sağlanmıştır.

*Örnek ölçek maddesi:*

*Randevularıma yetişmede rahatım 1 2 3 4 5 6 7 8 Hiçbir zaman geç kalmam*

Katılımcıların kendilerini yakın hissettikleri ifadeye göre rakamsal derecelendirmeleri istenmiştir. Puanların hesaplanmasında Toplam puan 3 ile çarpılarak 99 puan ve altı B Tipi kişilik, 100 puan ve üzeri A tipi kişilik olarak değerlendirilmiştir.

### Geçerlik ve Güvenirlik

A/B Kişilik Tipi ölçeğine ait Cronbach's Alpha değeri 0,602 (n=7) olarak tespit edilmiştir. Güvenirlik katsayısı 0,6-0,7 kabul edilebilir değer olarak ifade edilmektedir (Kılıç, 2016). Siber güvenlik farkındalığının ölçümlenmesi tek soru ile gerçekleştirilmiştir. Verilerin dağılımına ilişkin normallik testi sonuçları Tablo 2'de verilmiştir.

**Tablo 2.** *Normallik Testi*

| | ***Siber Güvenlik Farkındalığı*** | ***Cinsiyet*** | ***A / B Kişilik Tipi*** |
|---|---|---|---|
| *N* | *172* | *172* | *172* |
| *Skewness (Çarpıklık)* | *,184* | *,236* | *,432* |
| *Skewness'in Std. Hatası* | *,185* | *,185* | *,185* |
| *Kurtosis (Basıklık)* | *-,718* | *-1,967* | *-1,835* |
| *Kurtosis'in Std. Hatası* | *,368* | *,368* | *,368* |

Basıklık değerinin ±1.5 arasında olması kabul edilir bir değerdir (Tabachnick ve Fidell, 2013). Çarpıklık değerlerinin -1 ila +1 aralığının dışında kalması büyük ölçüde çarpık bir dağılıma işaret eder." (Hair, Black, Babin ve Anderson (2013). Verilere bakıldığında basıklık değerlerinin siber güvenlik farkındalığında -,718, cinsiyette -1,967, A ve B tipi kişilikte -1,835 olduğu görülmektedir. Değerin ±1.5 aralığında olmamasından dolayı verilerin normal dağılım göstermediği görülmektedir. Bu nedenle verilerin analizinde iki bağımsız grup arasındaki farkın önemini test etmek için Mann- Whitney testi kullanılmıştır.

### Verilerin Analizi

Verilerin analizinde SPSS Statistics 25 kullanılmıştır. Tanımlayıcı analiz ve iki bağımsız örneklem arasındaki farkın öneminin sınanması için Mann-Whitney Testi kullanılmıştır.

## Bulgular

Katılımcıların profilini ortaya koymak adına yapılmış olan frekans analizine ait tablolar aşağıda verilmiştir. Katılımcılar üniversitede öğrenim hayatına devam eden öğrencilerden oluşmaktadır. Katılımcılardan yalnızca cinsiyet bilgisinin öğrenilmiştir.

**Tablo 3:** *Demografik Bilgiler*

| **Değişken** | | | |
|---|---|---|---|
| | **Düzey** | **n** | **%** |
| Cinsiyet | Kadın | 96 | 55,8 |
| | Erkek | 76 | 44,2 |
| | Toplam | 172 | 100,0 |

Katılımcıların % 55,8'i kadın ve % 44,2'si erkek öğrencilerden oluşmaktadır.

**Tablo 4:** *Tanımlayıcı İstatistik- Kişilik Tipi*

| **Değişken** | | | |
|---|---|---|---|
| | **Düzey** | **n** | **%** |
| Kişilik Tipi | A | 104 | 60,5 |
| | B | 68 | 39,5 |
| | Toplam | 172 | 100,0 |

Katılımcıların kişilik tiplerini gruplamak adına % 60,5'inin A tipi kişiliğe sahip olduğu görülmektedir. % 39,5'i ise B Tipi kişiliğe sahiptir.

**Tablo 5:** *Tanımlayıcı İstatistik- Siber Güvenlik Farkındalığı*

| Siber Güvenlik Farkındalığı | | | |
|---|---|---|---|
| | | **Frekans** | **Yüzde** |
| Geçerli | Bilgisiz | 30 | 17,4 |
| | Az Bilgili | 70 | 40,7 |
| | Bilgili | 52 | 30,2 |
| | Çok İyi Bilgili | 20 | 11,6 |
| | Toplam | 172 | 100,0 |

Katılımcıların siber güvenlik terimine olan aşinalığının sorulduğu ve bunun siber güvenlik farkındalığı olarak ifade edildiği bu çalışmada % 40,7 oranında az bilgili oldukları sonucuna ulaşılmıştır.

**Tablo 6:** *A/B Kişilik Tipi Siber Güvenlik Farkındalığı Ortalaması*

| A/B Kişilik Tipi Siber Güvenlik Farkındalığı Ortalaması | | | | | |
|---|---|---|---|---|---|
| | **N** | **Minimum** | **Maksimum** | **Ortalama** | **Std. Sapma** |
| SGF-A | 104 | 1 | 4 | 2,52 | ,870 |
| SGF-B | 68 | 1 | 4 | 2,12 | ,907 |

Siber güvenlik farkındalığının kişilik tiplerine göre ortalamasına bakıldığında A kişilik tipine sahip bireylerin siber güvenlik farkındalığı ortalaması 2,52, B kişilik tipine sahip bireylerin siber güvenlik farkındalığı ortalaması 2,12 olarak tespit edilmiştir.

### A/B Kişilik Tipine Göre Siber Güvenlik Farkındalığı

Elde edilen bulgulara göre A/B kişilik tipine göre siber güvenlik farkındalığı arasında farklılık görülmektedir (U=2644,0, p<,05) Hesaplanan sıralı ortalamalarda görüldüğü üzere A kişilik tipine (95,08) sahip katılımcıların siber güvenlik farkındalığı ile B tipi kişiliğe (73,38) sahip katılımcıların siber güvenlik farkındalığından daha fazladır. $H_1$ hipotezi kabul edilmiştir. Analize ilişkin bulgular Tablo 7' de verilmiştir.

**$H_1$:** Siber güvenlik farkındalığı A/B Kişilik Tipine Göre anlamlı farklılık göstermektedir.

**Tablo 7:** *Mann Whitney U Testi İstatistikleri (Kişilik-Siber Güvenlik Farkındalığı)*

| | **Değişkenler** | **n** | **Sıra Ortalaması** | **Sıra Toplamı** | **U** | **p** |
|---|---|---|---|---|---|---|
| **Siber Güvenlik Farkındalığı** | A | 104 | 95,08 | 9888,00 | 2644.000 | ,003 |
| | B | 68 | 73,38 | 4990,00 | | |
| | Toplam | 172 | | | | |

Tablo 8 incelendiğinde; elde edilen bulgulara göre cinsiyete göre siber güvenlik farkındalığı arasında farklılık görülmektedir (U=2560,0, p<,05) Hesaplanan sıralı ortalamalarda görüldüğü üzere kadın (97,83) katılımcıların siber güvenlik farkındalığı ile erkek (72,18) katılımcıların siber güvenlik farkındalığından daha fazladır. $H_2$ hipotezi kabul edilmiştir.

**$H_2$:** Siber güvenlik farkındalığı cinsiyete göre anlamlı farklılık göstermektedir.

**Tablo 8:** *Mann Whitney U Testi İstatistikleri (Cinsiyet-Siber Güvenlik Farkındalığı)*

| | **Değişkenler** | **n** | **Sıra Ortalaması** | **Sıra Toplamı** | **U** | **p** |
|---|---|---|---|---|---|---|
| **Siber Güvenlik Farkındalığı** | Kadın | 96 | 97,83 | 9392,00 | 2560,000 | ,000 |
| | Erkek | 76 | 72,18 | 5486,00 | | |
| | Toplam | 172 | | | | |

Çalışmanın sonuçlarına göre katılımcılar arasında A kişilik tipine sahip ve kadın katılımcıların siber güvenlik farkındalığı daha yüksektir. Bunun bir sebebi olarak A kişilik tipine sahip bireylerin başarı odaklı ve işlerinde yavaşlıktan hoşlanmayan, hızlı düşünen ve işlerini hızlı bitiren ve diğer insanlar ile yarış halinde olan bireylerden oluşması olarak gösterilebilir. Siber güvenlik farkındalığı, bireylerin siber tehditler ve güvenlik önlemleri hakkında bilinçli olmaları ve bu konuda dikkatli davranmaları anlamına gelir. Bu farkındalık, kişilerin bilgi güvenliği önlemlerini alması, güçlü parolalar kullanması, güvenlik yazılımlarını güncel tutması, siber saldırılara karşı dikkatli olması ve bilgi paylaşımı konusunda özenli davranmasını gerektirmektedir. A tipi kişilik özelliklerine sahip bireyler, işlerinde belirli hedeflere odaklanma eğilimindedirler. Bu odaklanma, siber güvenlikle ilgili işlerin etkili bir şekilde yerine getirilmesine katkı sağlayabilir. Zira bu bireylerin hedeflere yönelik güçlü bir motivasyonu, işlerin siber güvenlik standartlarına uygun bir şekilde gerçekleştirilmesi konusunda artan bir farkındalık geliştirmelerine yardımcı olabilir.

## Tartışma, Sonuç ve Öneriler

Bireylerin sahip oldukları kişilik tipleri her alanda insan davranışını şekillendirmekte ve etkilemektedir. Çalışmanın odağında yer alan A/B kişilik tipine sahip üniversite öğrencilerinin siber güvenlik farkındalığındaki farklılığın ortaya konulması amaçlanmıştır. Farklı kişilik tipine sahip bireylerin farkındalıklarının şekillenmesi de değişmektedir. Farkındalık oluşumu bireyin kişiliğinden etkilenmektedir (Song ve Zhang 2022). Siber güvenlik farkındalığı her bireyin sahip olması gereken bilgi güvenliğini sağlayan önemli bir farkındalıktır. Siber güvenlik farkındalığı aynı zamanda siber güvenlik kültürünün oluşmasına da katkı sağlamaktadır. Siber güvenlik kültürü ise siber güvenlik ile ilgili tüm konuların örgütlerin kültürlerinin bir parçası haline gelmesi anlamına gelmektedir. Farkındalık beraberinde tutumları ve tutumlar ise devamında davranışları getirmektedir. Davranışların süreklilik haline gelmesi ise örgüt kültüründe yerini alan bir siber güvenlik kültürünün oluşumu sağlanmaktadır. Siber güvenlik örgütlerin karşılaştıkları ve göz ardı edemeyecekleri kadar önemli bir yere sahiptir. Özellikle işlerin dijital ortamda yoğunluklu olarak yapılması bilginin işlenmesi, saklanması ve güvenliğinin korunması konusunda azami bir özenin gösterilmesi gerekmektedir. Bu çalışma ise siber güvenlik konusunda bireylerin kişilik tiplerine göre gerekli özeni gösterip göstermediği konusunda ön bir araştırma olarak nitelendirilmektedir. Çalışmanın sonuçlarına bakıldığında; A kişilik tipine sahip katılımcıların siber güvenlik farkındalığının yüksek olduğu tespit edilmiştir**.** Bunun yanı sıra kadın katılımcıların ise siber güvenlik farkındalığı erkek katılımcılara göre yüksektir. Literatürde kişilik tipi ile siber güvenlik farkındalığının çalışıldığı bir araştırmaya rastlanılmamıştır. Fakat literatüre bakıldığında siber güvenlik farkındalığı ile yapılmış araştırmalar görülmüştür. Mohammad, vd. (2022) Siber güvenliğin önemine ilişkin farkındalığı etkin bir şekilde artırmak için biyolojik, psikolojik ve kültürel faktörler gibi kişi içi ve kişilerarası insan faktörlerinin bütünsel olarak ele alınması gerektiğini öne sürmüştür (Mohammad, Hussin, Husin, 2022). Yapılan bir diğer çalışmada ise mobil bankacılık kullanıcılarının siber güvenlik bilgisinin, siber güvenlik farkındalığını ve davranışsal seçim korumasını önemli ölçüde etkilediğini ortaya koymuştur. Ayrıca ulaşılan sonuçlar, siber güvenlik farkındalığının, davranışsal seçim korumasını önemli ölçüde etkilediğini ve siber güvenlik farkındalığının, siber güvenlik bilgisi ile davranışsal seçim koruması arasında önemli ölçüde aracılık ettiğini belirtmiştir (Limna, Kraiwanit ve Siripipattanakul, 2022). İleriki çalışmalarda siber güvenlik farkındalığının artırılması hususunda öneriler içeren ve kişilik tipinden kaynaklı bu farklılığın detaylıca araştırılması önerilmektedir. Kişilik tiplerine uygun olarak siber güvenlik farkındalığını artırıcı önlemlerin alınması ve bu konuda kişiliğe uygun farkındalığın dinamikliğini artıracak eğitim programlarının düzenlenmesi çalışma hayatına adım atacak üniversite öğrencileri için yararlı olacaktır. Özellikle yöneticilere kişilik tiplerine göre siber güvenlik farkındalığındaki bu farklılığın önüne geçmeye çalışmak ya da siber güvenlik farkındalığını artırmaya yönelik kampanya ve işbaşı eğitimlerin düzenlenmesi önerilmektedir. Bu çalışma sınırlı sayıda üniversite öğrencisinden elde edilen bilgiler doğrultusunda şekillendirilmiştir. Çalışmanın katılımcı sayısının az olması çalışmanın sonuçlarının genellenebilirliğini sınırlandırmaktadır. Çalışmayı diğer çalışmalardan ayıran bir husus ise siber güvenlik farkındalığı konusunda üniversite öğrencileri üzerine yapılmış çalışmalar bulunmasına rağmen hem siber güvenlik farkındalığı hem de kişilik tipine göre siber güvenlik farkındalığının bir arada ele alındığı bir çalışmaya rastlanılmamıştır. Bunun yanı sıra çalışma disiplinlerarası bir nitelik taşıdığı için hem siber güvenlik alanında hem de yönetim organizasyon alanında araştırma yapan bireyler için bir öncü niteliğindedir.

## Etik Beyan

*"A/B Kişilik Tipine Göre Siber Güvenlik Farkındalığı"* başlıklı çalışmanın yazım sürecinde bilimsel kurallara, etik ve alıntı kurallarına uyulmuş; toplanan veriler üzerinde herhangi bir tahrifat yapılmamış ve bu çalışma herhangi başka bir akademik yayın ortamına değerlendirme için gönderilmemiştir. Gerekli olan etik kurul izinleri Gümüşhane Üniversitesi Bilimsel Araştırma ve Yayın Etiği Kurulu'nun 28/07/2022 tarih ve 2022/5 sayılı toplantısında alınmıştır.

## Çatışma Beyanı

Çalışmada herhangi bir potansiyel çıkar çatışması söz konusu değildir.

## Kaynakça

Ahmed, N.; Li. C.; Khan, A.; Qalati, S.A.; Naz, S. & Rana, F. (2021). Purchase intention toward organic food among young consumersusing theory of planned behavior: role of environmental concernsand environmental awareness. *Journal of Environmental Planning and Management*, 64(5), 796-822, doi: 10.1080/09640568.2020.1785404.

Ajzen, I. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. In: Kuhl, J., Beckmann, J. (eds) Action Control. SSSP Springer Series in Social Psychology. Springer, Berlin, Heidelberg, 11-39.

Aksoğan, M., Bayer, H., Gülada, M. O., ve Çelik, E. (2018). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği. *Kesit Akademi Dergisi*, (13), 271-288. Erişim adresi: https://dergipark.org.tr/en/download/article-file/1519896

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia, *Heliyon*, 7(e06016), 1-13, doi: 10.1016/j.heliyon.2021.e06016.

Başarır, Ö. (2020). Marka farkındalığı ile satın alma niyeti arasındaki ilişki bağlamında televizyon dizilerinde ürün yerleştirme. *IBAD Sosyal Bilimler Dergisi*, (8), 383-403, doi: 10.21733/ibad.740021

Bilgin Yurdaöz, A. ve Cemaloğlu, N. (2021). Okul Yöneticilerin Gösterdiği A Tipi ve B Tipi Kişilik Özellikleri ile Öğretmenlerin Motivasyonları Arasındaki İlişki. *Recep Tayyip Erdoğan Üniversitesi Sosyal Bilimler Dergisi*, 8(14): 161-190. doi: 10.34086/rteusbe.1015798

Burger, J. M. (2015). *Personality* (9. b.). Stamford, USA: Cengage Learning.

Chang, L.Y.C. & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar, *Computers* & *Security*, 97(101959), 1-10, doi: 10.1016/j.cose.2020.101959.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (bilgi işlem daire başkanlıkları örneği). *Journal of Computer and Education Research*, 9(18), 598-625, doi: 10.18009/jcer.907022

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2013). *Multivariate Data Analysis*: Pearson Education Limited.

Huraj, L., Lengyelfalusy, T., Hurajová, A. & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal*, 12(2), 623-633, doi: 10.18421/TEM122-05, May 2023

İlter, İ. (2020). Akademik başarı, lisansüstü eğitim farkındalığı ve lisansüstü eğitim niyeti arasındaki ilişkiler, *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi*, 53(1), 117-156, doi: 10.30964/auebfd.582502.

Kılıç, S. (2016). Cronbach'ın alfa güvenirlik katsayısı. *Journal of Mood Disorders*, 6(1), 47-48 doi: 10.5455/jmood.20160307122823.

Kittel, F., Kornitzer, M., & Dramaix, M. (1986). Evaluation of type A personality. Postgraduate Medical Journal(62), 781-783. Erişim adresi: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2418837/pdf/postmedj00102-0064.pdf

Koçak, O.; Eti, S. Ve Gürsoy, G. (2017/2). A Ve B Kişilik Tipine Sahip Kamu Ve Özel Sektör Çalışanlarının Kişilik Tiplerinin İncelenmesi: Yalova Örneği, *HAK-İŞ Uluslararası Emek ve Toplum Dergisi*, 6,(15), 380-397. Erişim adresi: https://dergipark.org.tr/en/download/article-file/337656.

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The Relationship between Cyber Security Awareness, Knowledge, and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, doi: 10.25147/ijcsr.2017.001.1.123.

Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research* 2(3):173-191. Erişim adresi: https://www.jstor.org/stable/23010882

Mohammad, T., Hussin, N.A.M. & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. *Technology in Society*, 68 (101823), 1-8, doi: 10.1016/j.techsoc.2021.101823.

Rosenman, R. H., & Friedman, M. (1961). Association of specific behavior pattern in women with blood and cardiovascular findings. *Circulation*, 24(5), 1173-1184. Erişim adresi: https://www.ahajournals.org/doi/pdf/10.1161/01.CIR.24.5.1173

Song, D. & Zhang, Y. (2022) Opinion Formation on a Time Varying Dynamic Network with Different Personality Types: Stubborn, Follower, and Extreme. *5th Interna-tional Conference on Big Data Technologies* (ICBDT 2022), Qingdao, 23-25 September 2022, 190-195, doi: 10.1145/3565291.3565322.

Sönmez, K. (2022). Hemşirelerin Kişilik Özellikleri ile İşbirliği Niyetinin Planlı Davranış Teorisi Kapsamında İncelenmesi: Sağlık Kurumları Örneği, *Biruni Üniversitesi, Lisansüstü Eğitim Enstitüsü*, Doktora Tezi.

Tabachnick, B. G., &ve Fidell, L. S. (2013). *Using Multivariate Statistics* (6th ed.). Boston, MA: Pearson

TDK. (2022, 08). Türk Dil Kurumu Sözlükleri: https://sozluk.gov.tr/ adresinden alındı.

Trim, P.R.J. ve Lee, Y. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, 83, 224-238, doi: 10.1016/j.indmarman.2019.04.003.

Tuğal, İ., Almaz, C. ve Sevi, M., (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. *Bilişim Teknolojileri Dergisi*, 14(3), 229-238, doi: 10.17671/gazibtd.754458

Üçok, T. (2006). *Liderlik ve Yönetici Davranış Geliştirme*, Gazi Kitabevi, s.18.

Üzüm, B. ve Şenol, L. (2019). A-B kişilik tiplerinin presenteizme etkisi: Havacılık sektöründe bir araştırma. *OPUS– Uluslararası Toplum Araştırmaları Dergisi*, 11(18), 979-1000. doi: 10.26466/opus.552967.

Yıldız, G., & Özsoy, E. Çalışanların Kişilik Özelliğine Göre İş Doyumu Farklılaşır Mı? *Sosyal ve Beşeri Bilimler Dergisi*, 5(1), 268-278. Erişim adresi: https://dergipark.org.tr/en/download/article-file/117359

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, 62, doi: 10.1080/08874417.2020.1712269

## EXTENDED ABSTRACT

Cyber security is a reality that needs to be emphasized with the increase in digitalization and the increase in the population born into the digital age. Having cyber security awareness in both private and working life enables people to keep themselves and even their personal information safe. Recently, organizations want all their employees to have enough knowledge about cyber security. In the light of the Theory of Planned Behavior, analyzing the situation of cyber security awareness in university students who will start to take their place in business life will make a contribution to the literature. In addition, the problematic issue of the study is whether university students with personality type A or B show a difference in cyber security awareness. It is noticed that the research on type A and B personality classification focuses on the effects on behavioral outcomes according to personality types. This study, which deals with the difference in cybersecurity awareness in the perspective of the theory of planned behavior (Ajzen, 1985) of personality type, has the feature of being one of the pioneering studies that reveal to what extent personality types can adapt to these developments with technological developments and being a guide for future studies. Within the scope of the theory of planned behavior, it is thought that personality type can make a difference on an individual's cyber security awareness (van der Schyff & Flowerday, 2021). According to the Theory of Planned Behavior, 20-30% of individuals' behaviors can be explained by their intentions (Sönmez, 2022). According to PDT, the main element of individual behavior is intention. Behavioral intention should have three tendencies to perform the behavior. These are: attitudes towards behavior, subjective norm, perceived behavioral control. Some studies have revealed the effect of awareness on intention (Başarır, 2020; İlter, 2020). In another study, Mathieson (1991) compared the technology acceptance model and the theory of planned behavior to predict users' intentions to use an information system. The result of Mathieson's study showed that both models predict user intentions well and that although the technology acceptance model is the easiest theory to apply, the Theory of Planned Behavior provides more specific information. Harrison et al. (1997) used the Theory of Planned Behavior to explain and predict small business managers' decisions to adopt an information technology. They found that the Theory of Planned Behavior is useful in explaining the managers' decision process and that the decision process is a function of attitude toward adoption, subjective norm toward adoption, and perceived control over adoption. In this context, within the scope of the Theory of Planned Behavior, the effect of awareness on intention and the effect of intention on behavior is seen. The sample of the study was formed by snowball sampling method among university students studying at a state university. SPSS Statistics 25 was used to analyze the data. Descriptive analysis and Mann-Whitney Test were used to test the significance of the difference between two independent samples. As a result of the analysis of 172 participants; cyber security awareness has a statistically significant difference according to personality types A and B. In addition, cyber security awareness also showed a significant difference according to gender. The average cyber security awareness of the participants with type A personality was found to be 2.52. The average cyber security awareness of the participants with type B personality was found to be 2.12. According to the results of the study, the cyber security awareness of the participants with personality type A and female participants is higher. In future studies, it is recommended to investigate this difference due to personality type in detail, including suggestions for increasing cyber security awareness. In particular, it is recommended that managers try to prevent this difference in cyber security awareness according to personality types or organize campaigns and trainings to increase cyber security awareness. According to the results of the study, among the participants, the cyber security awareness of the participants with personality type A and female participants is higher. It is recommended that this difference due to personality type should be investigated in detail in future studies, including suggestions for increasing cyber security awareness. Awareness leads to attitudes and attitudes lead to behaviors. The continuity of behaviors ensures the formation of a cyber security culture that takes its place in the organizational culture. Cyber security has an important place that organizations face and cannot ignore. Especially when the work is done intensively in the digital environment, maximum care should be taken in processing, storing and protecting the security of information. In particular, it is recommended that managers try to prevent this difference in cyber security awareness according to personality types or organize campaigns and trainings to increase cyber security awareness.