Mesleki Eğitim Uzmanları için El Kitabı

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

31 MAYIS 2024

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Proje No: 2022-1-LV01-KA220-VET-000086725 | Proje başlığı: Girişimler için İyi Dijital Hijyen

İçindekiler

Modül 1 - Mesleki Eğitim ve Öğretim Profesyonelleri için Dijital Hijyen 5
Ünite 1 - Mesleki Eğitim ve Öğretimde Dijital Hijyenin Önemi 5
Dijital Hijyen ve Siber Güvenlik 5
Mesleki Eğitim ve Öğretim Kurumlarında Dijital Hijyen 5
Ünite 2- Mesleki Eğitim ve Öğretim Eğitmenleri için Beceriler ve Gereklilikler 8
Mesleki Eğitim ve Öğretim Kuruluşları için Rol ve Sorumluluklar 8
Dijital Beceri Çerçeveleri 10
Mesleki Eğitim ve Öğretim Eğitmenleri ve Eğitimciler için Beceriler 12
Ünite 3 - Dijital Hijyenin Mesleki Eğitim ve Öğretim Müfredatına ve Eğitimine Uyarlanması 15
Ünite 4 - İyi Uygulama Örneği - Mesleki Eğitim ve Öğretim Kurumları için Dijital Hijyen 18
Durum açıklaması 18
Çözüm 18
Kaynaklar 22
Modül 2 - Mesleki Eğitim ve Öğretim Kurumları için Özelleştirilmiş Dijital Hijyen Müfredatı 23
Giriş 23
Ünite 1 - Müfredata Genel Bakış 23
Modülün Program Amaç ve Hedefleri 24
Öğretim Metodolojisi 24
Değerlendirme ve Sürekli İyileştirme 24
Sonuç 25
Ünite 2 - Temel Öğrenme Alanları 26
Müfredata Genel Bakış 26
Dijital Hijyene Giriş 26
Ağ ve Siber Güvenlik 28
Veri ve Dosya Yönetimi 29
Yazılım Yönetimi 30
Veri Yedekleme ve Kurtarma 32

Kriptografi, Kimlik Doğrulama ve Parola Yönetimi 33
Mobil Cihaz Yönetimi ve Güvenliği 34
Ünite 3 - Mesleki Eğitim ve Öğretim Kurumları için Dijital Hijyen Değerlendirme ve Geri Bildirim Mekanizmaları 36
Giriş 36
Değerlendirme Stratejileri 36
Geri Bildirim Mekanizmaları 37
Geri Bildirimin Müfredat Gelişimine Uygulanması 37
Sonuç 38
Ünite 4 - Mesleki Eğitim ve Öğretim Kurumlarından İyi Uygulamalar 39
Giriş 39
Örnek Çalışma 1: CyberVET Akademisi 39
Örnek Çalışma 2: TechBridge Mesleki Eğitim ve Öğretim 40
Örnek Çalışma 3: SecurePath Enstitüsü 40
En İyi Uygulamalar için Çıkarımlar 41
Örnek Çalışma 4: DigitalDefenders College 41
Örnek Çalışma 5: InnovateTech Enstitüsü 42
İyi Uygulamaların Özeti 42
Sonuç 43
Önemli Çıkarımlar ve En İyi Uygulamalar 43
Kaynaklar: 45
Modül 3: Uygulama ve Sürdürme 48
Ünite 1 - Girişimlerde ve Mesleki Eğitim Kurumlarında Dijital Hijyen Kültürü Oluşturma 48
Dijital Hijyen Kültürü Nedir? 48
Liderlik Kademesinde Dijital Hijyen Kültürünün Geliştirilmesi 48
Grup Düzeyinde Dijital Hijyen Kültürünün Geliştirilmesi 49
Bireysel Düzeyde Dijital Hijyen Kültürünün Geliştirilmesi 50
Ünite 2 - Dijital Hijyen Uygulamalarının İzlenmesi, Gözden Geçirilmesi ve Sürekli İyileştirilmesi 53

Kurumsal Düzeyde Uygulamalar 53
Bireysel Düzeyde Uygulamalar 55
Ünite 3 - Dijital Hijyenin Geleceği: Zorluklar ve Fırsatlar 57
A-Yükselen Teknolojiler 57
B-Düzenleyici Zorluklar 58
C-İnovasyon için Fırsatlar 59
Ünite 4 - Dijital Hijyen Kültürü İyi Uygulama Kullanım Örneği: 61
Dünya Çapında Dijital Hijyen Kullanım Örnekleri 61
Kaynaklar 64

Modül 1- Mesleki Eğitim ve Öğretim Profesyonelleri için Dijital Hijyen

Ünite 1- Mesleki Eğitim ve Öğretimde Dijital Hijyenin Önemi

Dijital Hijyen ve Siber Güvenlik

Dijital hijyen, bireylerin çevrimiçi gizliliklerini, güvenliklerini ve genel refahlarını korumak için kullandıkları uygulamaları ve alışkanlıkları ifade eder. Kişisel bilgilerin korunmasını, çevrimiçi tehditlerin önlenmesini ve dijital faaliyetlerle ilişkili risklerin en aza indirilmesini amaçlayan çok çeşitli proaktif davranışları ve önlemleri kapsar. Dijital hijyen uygulamalarına örnek olarak güçlü parolalar kullanmak, iki faktörlü kimlik doğrulamayı etkinleştirmek, yazılımı düzenli olarak güncellemek, kişisel bilgileri çevrimiçi paylaşma konusunda dikkatli olmak ve kişinin dijital ayak izini yönetmek verilebilir. Dijital hijyen, başka bir kavramla, yani siber güvenlikle yakından ilişkili bir kavramdır. Genellikle dijital hijyen, siber güvenliğin bireyin sorumluluğunda olan proaktif bir unsuru olarak kabul edilir.

Siber güvenlik, bilgisayar sistemlerini, ağları ve verileri yetkisiz erişimden, siber saldırılardan ve diğer güvenlik ihlallerinden korumaya adanmış özel bir alandır. Dijital varlıkları korumak ve çeşitli siber tehditlerin yarattığı potansiyel riskleri azaltmak için teknik önlemlerin, güvenlik protokollerinin ve savunma stratejilerinin uygulanmasını içerir. Siber güvenlikten sorumlu kişiler genellikle sistemlerdeki güvenlik açıklarını tespit etmek, güvenlik çözümleri geliştirmek, şüpheli faaliyetleri izlemek ve bilgi ve kaynakların bütünlüğünü, gizliliğini ve kullanılabilirliğini sağlamak için güvenlik olaylarına müdahale etmek için çalışırlar. Sonuç olarak, siber güvenlik faaliyetleri genellikle herkesin sorumluluğunda olabilecek dijital hijyenin aksine profesyoneller tarafından gerçekleştirilir.

Mesleki Eğitim ve Öğretimde Dijital Hijyen Kuruluşlar

Çeşitli kuruluşlar, dijital hijyen kurallarına ve en iyi uygulamalarına uyulduğundan emin olmak için çalışanlarından bazı genel kurallara uymalarını bekleme eğilimindedir. Mesleki eğitim ve öğretim (MEÖ) kuruluşları, insanlarla ve onların kişisel bilgileriyle ve dijital ortamda geliştirilen, depolanan ve paylaşılan özel hizmet ve ürünlerle çalışan tüm kuruluşlar için geçerli olan bazı genel kurallara sahiptir. Bununla birlikte, sundukları hizmetin türü ve hedef müşterilerinin benzersiz doğası ile ilgili bazı özel zorlukları vardır. Eğitimciler genellikle kendilerini müşterilerine ek rehberlik sağlamaları gereken bir durumda bulurlar. Bu,

eğitimi gerçekleştirirken, örneğin amaçlanan hizmeti sunarken dijital hijyen aracıları olmaları gerektiği anlamına gelebilir.

Dijital hijyenin özellikle MEÖ kuruluşları için çok önemli görülmesinin birkaç nedeni vardır:

- **Hassas bilgilerin korunması**

Mesleki Eğitim ve Öğretim kuruluşları işlerini yaparken genellikle öğrenci kayıtları, akademik veriler ve finansal ayrıntılar da dahil olmak üzere çok sayıda hassas bilgiyi ele alır. Bu bilgilerin bazıları, öğrenme analitiği gerçekleştirirken veya müşterilere sağlanan hizmetleri değerlendirirken kuruluş için çok önemli olabilir. İyi bir dijital hijyen uygulaması, bu bilgilerin yetkisiz erişime, veri ihlallerine ve siber tehditlere karşı korunmasına yardımcı olarak hassas verilerin gizliliğini ve bütünlüğünü sağlar.

- **Kurumsal itibarın korunması**

Bir MEÖ kuruluşuna emanet edilen verileri uygun düzeyde özen göstermeden ele alan kuruluş, istemeden de olsa müşterilerinin ve ortaklarının kendisine bakış açısını değiştirebilir. Bir veri ihlali veya güvenlik olayı, bir Mesleki Eğitim ve Öğretim kurumuna itibar açısından önemli zararlar verebilir. Kurumlar dijital hijyen uygulamalarına öncelik vererek güvenlik, güvenilirlik ve profesyonellik konusundaki kararlılıklarını göstermekte ve böylece öğrenciler, veliler, işverenler ve düzenleyici kurumlar da dahil olmak üzere paydaşlar nezdindeki itibarlarını artırmaktadır.

- **Yönetmeliklere uygunluk**

Mesleki eğitim ve öğretim kuruluşları, işlerinin niteliğine ve müşterileriyle nasıl bağlantı kurduklarına bağlı olarak veri koruma, gizlilik ve siber güvenlikle ilgili çeşitli düzenlemelere ve uyumluluk gerekliliklerine tabidir. En iyi dijital hijyen uygulamalarına bağlı kalmak, ilgili yasa ve yönetmeliklerle uyumluluğun sağlanmasına yardımcı olur ve uyumsuzlukla ilişkili yasal para cezaları, cezalar ve yasal yükümlülükler riskini azaltır.

- **Öğrenme ve öğretme için destek**

Dijital teknolojiler, çevrimiçi öğrenmeyi, işbirliğine dayalı projeleri ve dijital değerlendirmeleri kolaylaştırarak modern eğitimde çok önemli bir rol oynamaktadır. Bu teknolojiler eğitim materyalleri geliştirmek, yönetmek ve paylaşmak, eğitim ortamları düzenlemek, katılımcıların bunlara katılımını yönetmek veya eğitim sürecinde toplanan verileri analiz etmek için kullanılır. Mesleki eğitim ve öğretim kuruluşları, güvenli ve güvenilir bir dijital altyapı sağlayarak öğrenciler ve eğitimciler için sorunsuz bir öğrenme deneyimi sunabilir, inovasyonu, yaratıcılığı ve öğretme ve öğrenme faaliyetlerine katılımı teşvik edebilir.

- **Siber güvenlik risklerinin azaltılması**

Eğitim sektörü, dijital sistem ve ağlardaki açıklardan ya da dijital ortamda eğitim almaya alışkın olmayan öğrenci ve eğitmenlerin bilgi ve beceri eksikliklerinden faydalanmak isteyen siber suçluların hedefi olabilir. Dijital hijyen önlemlerinin uygulanması, kötü amaçlı yazılım enfeksiyonları, kimlik avı saldırıları, fidye yazılımı

tehditleri ve eğitim kaynaklarına yetkisiz erişim dahil olmak üzere siber güvenlik risklerinin azaltılmasına yardımcı olur ve böylece eğitim hizmetlerinin ve operasyonlarının sürekliliğini korur.

- **Sorumlu dijital vatandaşlığın teşvik edilmesi**

Sürecin bazı katılımcıları için bu, dijital bir ortamda yürütülen veya eğitim materyalleri oluşturmak, yönetmek ve paylaşmak için dijital bir ortam kullanan, bilgi paylaşımı ve diğer katılımcılarla dijital yollarla iletişim kuran veya eğitim sırasında idari görevleri yerine getirmek için dijital araçlar kullanan bir eğitim biçimine dahil olmak için ilk fırsat olabilir. Mesleki eğitim ve öğretim kuruluşları, eğitimde yer alan öğrencilerini ve personelini güvenli ve sorumlu dijital uygulamalar konusunda eğitme sorumluluğuna sahiptir. Dijital hijyen eğitimini Mesleki Eğitim ve Öğretim müfredatına ve eğitim programlarına entegre ederek kurumlar, öğrencileri dijital ortamda etkili bir şekilde gezinmek, çevrimiçi kimliklerini korumak ve dijital topluma olumlu katkıda bulunmak için gereken bilgi, beceri ve tutumlarla güçlendirir.

- **Gelecekteki kariyerler için hazırlık**

Günümüz dijital çağında, dijital okuryazarlık ve siber güvenlik farkındalığı, işgücüne katılan bireyler için temel becerilerdir. Dijital hijyenle ilgili bazı becerileri öğrenmek bir öğrencinin ana hedefi olmasa da, eğitime katılım onlara gelecekte faydalı olabilecek bu becerileri geliştirme fırsatları sağlayabilir. Eğitmenler ve eğitim organizatörleri de bu özel amaç için zaman ve kaynak ayırma ihtiyacı olabileceğinin farkında olmalıdır. Mesleki eğitim ve öğretim kurumları, dijital hijyen uygulamalarını teşvik ederek öğrencileri, ister geleneksel ister dijital sektörlerde olsun, gelecekteki kariyerlerinde dijital zorlukların üstesinden gelebilmeleri için gereken temel bilgi ve becerilerle donatmaktadır. Aynı durum, dijital ortamları ve araçları güvenli ve sorumlu bir şekilde kullanarak eğitime katılarak öğretim uygulamalarını modern tutan ve kariyerleri için yeni fırsatlarla karşılaşabilecek eğitmenler için de geçerlidir.

Genel olarak, dijital hijyen, hassas bilgileri korumak, kurumsal itibarı korumak, düzenlemelere uymak, öğrenmeyi ve öğretmeyi desteklemek, siber güvenlik risklerini azaltmak, sorumlu dijital vatandaşlığı teşvik etmek ve öğrencileri ve bir dereceye kadar eğitmenlerini ve diğer çalışanları dijital bir dünyada başarıya hazırlamak için şirket düzeyinde MEÖ kuruluşları için olduğu kadar bireysel bir çalışan ve müşteri düzeyinde de önemlidir. Mesleki eğitim ve öğretim kurumları, dijital hijyene öncelik vererek öğrencilerin dijital çağda başarılı olmalarını sağlayan güvenli, emniyetli ve elverişli bir öğrenme ortamı yaratabilir.

Ünite 2- Mesleki Eğitim ve Öğretim Eğitmenleri için Beceriler ve Gereklilikler

Mesleki Eğitim ve Öğretim Kuruluşları için Rol ve Sorumluluklar

İlk olarak, dijital hijyen konularının farkında olması ve ilgili becerilere sahip olması gereken MEÖ eğitimine dahil olan rollerin kimler olabileceği ile başlayalım. Mesleki eğitim ve öğretim eğitmenleri ve eğitimcileri, dijital ortamlarda ve dijital araçlar kullanılarak gerçekleştirilen eğitimleri yürütürken ve bunlara katılırken durumlara bağlı olarak, sürecin katılımcıları tarafından gerçekleştirilen bireysel görevlerin farklı bölümleriyle karşılaşabilirler. Bu nedenle, bir mesleki eğitim ve öğretim (VET) kurumunda dijital hijyenin uygulanması ve yönetilmesi, farklı rol ve sorumluluklara sahip çeşitli paydaşlar arasında koordinasyon ve işbirliği gerektirebilir. Eğitmenler, eğitimin teknik yönleriyle ilgilenmek için tam donanımlı bir BT personeli tarafından desteklenme lüksüne sahip olabilir veya kendi beceri ve bilgilerine güvenmek zorunda kalabilirler. Bu nedenle, Mesleki Eğitim ve Öğretim eğitmenleri ve eğitimcileri için beceriler ve gereksinimler, parçası oldukları kuruluşa bağlı olarak değişebilir.

Günümüzün dijital ortamında sürece veya eğitime dahil olabilecek bireyler için her biri kendi görev ve beceri gereksinimlerine sahip çeşitli tipik roller ve sorumluluklar vardır:

- **Baş Bilgi Yetkilisi (CIO) veya Baş Teknoloji Yetkilisi (CTO)**

CIO veya CTO esas olarak kuruluşun dijital hijyen stratejisini, politikalarını ve prosedürlerini geliştirmek ve denetlemekle ilgilenir. Dijital hijyen ve siber güvenlik göz önünde bulundurularak kuruluşlar için hedeflerin belirlenmesine katılırlar. Sorumlulukları arasında dijital hijyen çabalarının kurumun genel BT ve güvenlik hedefleriyle uyumunun sağlanması, dijital hijyen girişimleri ve siber güvenlik önlemleri için kaynak ve bütçe ayrılması ve dijital hijyen uygulamalarının hayata geçirilmesinden sorumlu BT ve güvenlik ekiplerine liderlik ve rehberlik sağlanması yer alır.

- **BT Güvenlik Müdürü veya Siber Güvenlik Sorumlusu**

Bazı kurumlarda BT Güvenlik yöneticisi veya siber güvenlik görevlisi gibi özel bir pozisyon veya iş tanımının bir parçası olarak bu rolü yerine getiren biri olabilir. Böyle bir rol, MEÖ sistemlerini, ağlarını ve verilerini korumak için siber güvenlik kontrolleri, koruma önlemleri ve risk yönetimi tedbirleri tasarlar ve uygular. Ayrıca, potansiyel tehditleri ve güvenlik açıklarını belirlemek ve azaltmak, güvenlik olaylarını izlemek, siber güvenlik olaylarına müdahale etmek ve olay müdahale faaliyetlerini koordine etmek için düzenli güvenlik değerlendirmeleri, denetimler ve güvenlik açığı taramaları yaparlar. Zaman zaman bu rol, personel için siber güvenlik eğitimi ve farkındalık programları geliştirir ve sunar, bu da onları bir MEÖ eğitmeni rolünü üstlenmelerini sağlar. Bazen de uzman olarak kendi kurumları dışında iyi dijital hijyen uygulamalarını teşvik etmek üzere öğrencileri eğitmeye davet edilebilirler.

- **BT Yöneticisi veya Sistem Yöneticisi**

BT yöneticileri kurumun BT altyapısını yönetmekten sorumludur ve bazen arka planda fark edilmeden MEÖ eğitmenleri için bazı görevleri tamamlayabilirler. Sorumlulukları arasında dijital hijyen standartlarını ve en iyi uygulamaları izleyerek VET sistemlerini, sunucularını ve ağ altyapısını korumak ve yönetmek; VET kaynaklarına ve verilerine güvenli erişim sağlamak için kullanıcı hesaplarını, erişim kontrollerini ve izinlerini yönetmek; dijital araçları kullanırken karşılaşılabilecek bilinen güvenlik açıklarına ve istismarlara karşı koruma sağlamak ve eğitim sırasında eğitim materyallerini paylaşmak veya katılımcılar arasında iletişim kurmak gibi eylemleri gerçekleştirmek için güvenlik yazılımını, yamaları ve bellenimi yüklemek, yapılandırmak ve güncellemek yer alır. Ayrıca şüpheli faaliyetler, yetkisiz erişim girişimleri veya güvenlik ihlalleri için sistem günlüklerini ve uyarılarını izlemekten de sorumludurlar.

- **Veri Koruma Görevlisi (DPO) veya Gizlilik Görevlisi**

Veri koruma görevlileri, MEÖ kuruluşlarının eğitim katılımcılarının hassas verilerini nasıl yönettiğine dikkat edilmesini gerektiren ulusal ve uluslararası düzeyde kurallar ve düzenlemeler olduğundan MEÖ'de önemli bir rol oynamaktadır. Bu rol, MEÖ ortamlarında kişisel verilerin toplanması, kullanılması ve saklanmasını düzenleyen veri koruma yönetmeliklerine ve gizlilik yasalarına uyulmasını sağlar; veri koruma etki değerlendirmeleri (DPIA'lar) ve gizlilik bildirimleri dahil olmak üzere veri koruma politikaları, prosedürleri ve belgeleri geliştirir ve sürdürür; veri koruma ve gizlilik uygulamalarıyla ilgili veri sahibi erişim taleplerini, gizlilik şikayetlerini ve sorgularını ele alır, veri güvenliği olaylarını, ihlallerini ve gizlilik ihlallerini ele almak için BT ve hukuk ekipleriyle işbirliği yapar.

- **Eğitim Teknoloğu veya Öğretim Tasarımcısı**

Önceki rollere herhangi bir kuruluşta rastlanabilse de, eğitim teknoloğu veya öğretim tasarımcısı kuruluş tarafından gerçekleştirilen eğitim ve öğretimle doğrudan ilgilidir. Sorumlulukları arasında dijital hijyen ilke ve uygulamalarının MEÖ müfredatına, öğretim materyallerine ve öğrenme faaliyetlerine entegre edilmesi; dijital hijyen eğitiminin öğretim uygulamalarına dahil edilmesi konusunda eğitimcilere ve öğretim personeline eğitim ve destek sağlanması, MEÖ öğrencileri için güvenlik, gizlilik ve erişilebilirliğe öncelik veren eğitim teknolojisi araçlarının ve kaynaklarının değerlendirilmesi ve önerilmesi yer almaktadır.

- **Son Kullanıcılar (Personel ve Öğrenciler)**

Son rol genellikle iki gruba ayrılır, ancak her ikisinin de dijital hijyen açısından benzer sorumlulukları vardır. Son kullanıcıların MEÖ sistemlerini, cihazlarını ve çevrimiçi kaynaklarını kullanırken dijital hijyen politikalarına, yönergelerine ve en iyi uygulamalara uymaları beklenir. Kuruluşun eğitim personelinin, kuruluşun kuralları ve politikası tarafından belirlenen belirli bir şekilde eğitim veya idari faaliyetler gerçekleştirmesi şirket tarafından istenebilir. Bu nedenle, dijital riskler ve sorumluluklar konusundaki anlayışlarını geliştirmek için siber güvenlik farkındalık eğitimi ve eğitim girişimlerine katılmaları ve güvenlik

olaylarını, şüpheli faaliyetleri ve siber güvenlik endişelerini soruşturma ve çözüm için uygun BT veya güvenlik personeline bildirmeleri gerekebilir. Bununla birlikte, MEÖ eğitmenleri, eğitim sırasında aşina olmayabilecekleri dijital bir ortamı kullanırken rehberliğe ihtiyaç duyabilecek öğrencilere danışman olarak rollerinin farkında olmalıdır.

Bir Mesleki Eğitim ve Öğretim kuruluşundaki bir birey, eğitim sırasında aynı anda birkaç rolü yerine getirebilir veya yalnızca birkaç sorumluluğa odaklanabilir. Ne olursa olsun, bir MEÖ kurumunda dijital hijyenin uygulanması ve yönetilmesinde yer alan bireyler için net roller ve sorumluluklar tanımlayarak, kurumlar bir siber güvenlik farkındalığı kültürü oluşturmak, iyi dijital hijyen uygulamalarını teşvik etmek ve MEÖ kaynaklarının ve verilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için etkili bir şekilde işbirliği yapabilir. Bununla birlikte, kurumlar yukarıda belirtilen uygulamaları gerçekleştirmek için bu kişilerin belirli beceri ve bilgilere sahip olmasını gerektirecektir.

Dijital Beceri Çerçeveleri

Dijital ortamda çeşitli faaliyetler gerçekleştiren kişilerin sahip olması gereken becerileri tanımlamak için oluşturulmuş mevcut yeterlilik çerçeveleri bulunmaktadır. Bunlardan bazıları genel dijital becerileri içerirken bazıları siber güvenlik ve dijital hijyen konuları için daha spesifik olabilir. Aşağıdaki çerçeveler, mesleki eğitim ve öğretim eğitmenleri ve eğitimcileri için dijital hijyen becerilerinin belirlenmesinin yanı sıra dijital ortamda eğitime katılan öğrenciler için olası eğitim ihtiyaçlarının belirlenmesinde yardımcı olmaktadır.

- **Vatandaşlar için Dijital Yetkinlik Çerçevesi (DigComp) [1]**

Avrupa Komisyonu tarafından geliştirilen DigComp 2.2 çerçevesi, Vatandaşlar için Dijital Yeterlilik Çerçevesinin en yeni versiyonudur. Dijital yetkinliğin temel bileşenlerini beş alanda tanımlamaktadır: Bilgi ve veri okuryazarlığı, İletişim ve işbirliği, Dijital içerik oluşturma, Güvenlik ve Problem çözme. Her alan ayrıca dijital ortamlarda yetkin olmak için gereken beceri ve bilgileri tanımlayan belirli yetkinliklere ayrılmıştır.

Bu çerçeve, bireylerin dijital becerilerini değerlendirip geliştirmeleri ve eğitimciler ile politika yapıcıların dijital eğitim ve öğretimi destekleyen müfredat ve politikalar tasarlamaları için bir rehber görevi görmektedir. DigComp 2.2 ayrıca yeterlilik seviyeleri ve kullanım örnekleri sunarak çeşitli eğitim ve profesyonel ortamlar için pratik hale getirmektedir. Çerçeve, dijital bir toplumda etkin ve eleştirel bir şekilde çalışabilmenin önemini vurgulamaktadır.

- **Avrupa e-Yetkinlik Çerçevesi (E-CF) [2]**

Avrupa e-Yetkinlik Çerçevesi (e-CF), Bilgi ve İletişim Teknolojisi (BİT) profesyonellerinin yetkinliklerini, becerilerini ve yeterlilik seviyelerini tanımlamak için standartlaştırılmış bir çerçevedir ve BİT profesyonellerinin büyümesini ve hareketliliğini desteklemek için geliştirilmiştir. Çerçeve, Planla, Oluştur,

Çalıştır, Etkinleştir ve Yönet gibi BİT ile ilgili beş yetkinlik alanından oluşmaktadır. Toplamda 41 yetkinlik içermekte ve Temel'den Uzman'a kadar her seviyede bilgi, beceri ve özerkliği tanımlayan yeterlilik seviyelerini içermektedir. Ayrıca yetkinliklerle ilgili bilgi ve beceri örneklerini de içermektedir.

e-CF, kurumların, İK yöneticilerinin, eğitmenlerin ve eğitimcilerin BİT profesyonelleri için iş rolleri ve kariyer yolları geliştirmelerine, işgücü yönetimini geliştirmelerine ve BİT sektöründe mesleki gelişimi teşvik etmelerine yardımcı olmayı amaçlamaktadır. Ayrıca Avrupa'nın dijital pazarında politika geliştirme, eğitim ve öğretim uyumu için bir araç olarak hizmet vermektedir.

- **Avrupa Siber Güvenlik Becerileri Çerçevesi (ECSF) [3]**

Avrupa Siber Güvenlik Becerileri Çerçevesi (ECSF), Avrupa genelinde siber güvenlik becerilerini, rollerini ve yetkinliklerini uyumlu hale getirmek ve standartlaştırmak için tasarlanmıştır. Siber güvenlik becerilerinin geliştirilmesi ve değerlendirilmesi için temel bir yapı olarak hizmet vermekte, siber güvenlik beceri boşluklarını ele almayı ve kuruluşların ve ulusların siber güvenlik duruşunu iyileştirmeyi amaçlamaktadır. ECSF, siber güvenlik becerilerini çeşitli alanlara ayırarak siber güvenlik alanında gerekli olan belirli rolleri ve yetkinlikleri detaylandırmaktadır. Kuruluşlar tarafından tipik olarak ihtiyaç duyulan temel siber güvenlik rollerini, bu rollerde etkili bir şekilde performans göstermek için gereken belirli becerileri ve yetenekleri ve her bir yetkinlik için gerekli olan başlangıç seviyesinden uzmanlığa kadar yeterlilik seviyelerini veya uzmanlık düzeylerini ana hatlarıyla belirtir.

Bu çerçeve, eğitim kurumları, şirketler ve politika yapıcılar da dahil olmak üzere çeşitli paydaşların siber güvenlik alanında müfredat, eğitim programları ve kariyer yolları geliştirmeleri için faydalıdır. Siber güvenlik alanında net kariyer yapılarının oluşturulmasını destekleyerek beceri eksikliklerinin belirlenmesini ve etkin bir şekilde ele alınmasını kolaylaştırır.

- **Eğitimciler için Dijital Yetkinlik Çerçevesi (DigCompEdu) [4]**

DigCompEdu çerçevesi, eğitimcilerin dijital yetkinlik gelişimi için gereklilikleri tanımlamaktadır. Erken çocukluktan yüksek ve yetişkin eğitime kadar tüm eğitim seviyelerindeki öğretmenler için özel olarak tasarlanmıştır ve giderek artan dijital öğrenme ortamlarında etkili öğretim için gerekli dijital becerileri geliştirmeye odaklanmaktadır. Çerçeve, mesleki katılım (İletişim, işbirliği ve mesleki gelişim için dijital teknolojilerin kullanılması), dijital kaynaklar (Dijital kaynakların oluşturulması, değiştirilmesi ve etkili bir şekilde yönetilmesi), öğretme ve öğrenme (Öğretme ve öğrenme sürecinin hazırlanması, uygulanması ve yönetilmesi için dijital teknolojilerin kullanılması), değerlendirme (Öğretme ve öğrenme sürecinin hazırlanması, uygulanması ve yönetilmesi için dijital teknolojilerin kullanılması) olmak üzere altı yeterlilik alanı etrafında yapılandırılmıştır.), değerlendirme (Öğrenmenin değerlendirilmesi için dijital teknolojilerden yararlanma.), öğrencileri güçlendirme (Kapsayıcılığı, kişiselleştirmeyi ve öğrencilerin aktif katılımını artırmak

için dijital araçları kullanma.), öğrencilerin dijital yeterliliğini kolaylaştırma (Öğrencilerin dijital becerilerini ve dijital araçların güvenli ve sorumlu kullanımını stratejik olarak teşvik etme.) Ayrıca DigCompEdu çerçevesi, eğitimcilerin dijital uygulamalarındaki gelişimleri için bir yol sağlayarak "Yeni Gelen "den "Öncü "ye kadar değişen 22 bireysel yetkinlik ve yeterlilik seviyesini tanımlamaktadır.

Bu çerçeve, eğitimcilerin dijital yetkinliklerini değerlendirmeleri ve geliştirmeleri için bir rehber görevi görmekte ve eğitim kurumlarını çağdaş eğitim ihtiyaçları ile uyumlu eğitim programları ve politikaları tasarlama konusunda desteklemektedir.

Yukarıda bahsedilen çerçeveler, dijital ortamda herhangi bir uygulamaya katılan bireylerin ve kuruluşların gereksinimlerini belirlemeye yönelik genel olmakla birlikte, Mesleki Eğitim ve Öğretim eğitmenleri ve eğitimcilerinden istenen becerilerin kapsamına ilişkin yapılandırılmış bir görüş sağlar.

Mesleki Eğitim ve Öğretim Eğitmenleri ve Eğitimciler için Beceriler

Mesleki eğitim ve öğretim eğitmenleri ve eğitmenleri bir dereceye kadar dijital ortamdaki diğer katılımcılardan farklı değildir. Bu nedenle, iyi dijital hijyen uygulamalarına uymak için ihtiyaç duydukları beceriler, herkesin sahip olması gereken becerilerdir. Bu beceriler bir dizi teknik, davranışsal ve bilişsel yeteneği kapsar. Bunlar aynı zamanda modern veya geleceğin becerileri olarak adlandırılabilecek becerilerin bir alt kümesidir ve dijital ortamın son dönemdeki gelişimine bağlı olarak, bulut teknolojilerini kullanmak, büyük veriyi analiz etmek ve iş üretkenliğini ve verimliliğini artırmak için yapay zeka araçlarını kullanmak gibi kuruluşlar veya yakın gelecek için çok önemli olan beceriler olarak vurgulanan becerilerle aynıdır [5,6].

Ancak, yaptıkları işin doğası gereği, Mesleki Eğitim ve Öğretim eğitmenleri ve eğitmenlerinin verileri nasıl ele aldıklarına ve eğitim sürecindeki diğer katılımcılarla nasıl etkileşimde bulunduklarına daha fazla dikkat etmeleri gerekmektedir. İşte Mesleki Eğitim ve Öğretim eğitmenleri ve eğitimcileri için iyi dijital hijyen konusunda ihtiyaç duyulan bazı önemli beceriler:

- **Genel siber güvenlik farkındalığı**

Bu beceri, kötü amaçlı yazılım, kimlik avı ve sosyal mühendislik saldırıları gibi yaygın çevrimiçi tehditleri anlamayı ve bunları nasıl tanıyıp yanıtlayacağını bilmeyi; şüpheli web sitelerinden kaçınmak, güvenli bağlantılar (HTTPS) kullanmak ve dosya indirirken veya bağlantılara tıklarken dikkatli olmak dahil olmak üzere internette nasıl güvenli bir şekilde gezinileceğini bilmeyi içerir.

- **Veri koruma ve gizlilik**

Bu beceri, hassas verileri hem aktarılırken hem de beklerken şifreleyebilmeyi ve gerektiğinde verilerin nasıl güvenli bir şekilde silineceğini veya imha edileceğini bilmeyi; kişisel bilgilerin paylaşımını kontrol etmek için çeşitli çevrimiçi platformlarda ve cihazlarda gizlilik ayarlarının nasıl yapılandırılacağını anlamayı içerir.

- **Cihaz güvenliği ve yönetimi**

Bu beceri, güvenlik açıklarını yamamak ve bilinen istismarlara karşı korumak için yazılım, işletim sistemleri ve uygulamaları düzenli olarak güncelleme uygulamasını; farklı hesaplar için güçlü, benzersiz parolalar oluşturma ve parolaları güvenli bir şekilde saklamak ve yönetmek için parola yönetim araçlarını etkili bir şekilde kullanma becerisini; çevrimiçi hesaplara ekstra bir güvenlik katmanı eklemek için mevcut olduğunda çok faktörlü kimlik doğrulamayı etkinleştirme ve yönetme uygulamasını içerir.

- **Güvenli dijital iletişim**

Bu beceri, gizli bilgileri paylaşırken veya öğrencilerle, akranlarla, meslektaşlarla veya MEÖ kuruluşu dışındaki ortaklarla iletişim kurarken şifreli e-posta hizmetlerini kullanmak veya güvenli mesajlaşma uygulamalarını seçip kullanmak gibi güvenli iletişim uygulamalarını uygulamayı; MEÖ sistemlerini tehlikeye atabilecek veya veri ihlallerine yol açabilecek kimlik avı e-postalarını, dolandırıcılıkları ve diğer sosyal mühendislik taktiklerini belirleme ve bunlardan kaçınma yönergelerine uymayı içerir.

- **Dijital ayak izi yönetimi**

Bu beceri, kişinin dijital ayak izinin etkilerini anlamayı ve kişisel bilgilerin çevrimiçi ortamda açığa çıkmasını en aza indirmek için adımlar atmayı içerir; eğitime katılanlara da aynısını yapmalarını tavsiye eder.

- **Eleştirel düşünme**

Bu beceri, çevrimiçi kaynakların güvenilirliğini değerlendirmek, yanlış bilgileri ve dolandırıcılıkları tespit etmek ve eğitim yürütürken veya eğitime hazırlanırken çevrimiçi etkinlikler hakkında bilinçli kararlar vermek için eleştirel düşünme becerilerini geliştirmeyi ve uygulamayı içerir.

- **Sürekli öğrenme**

Bu beceri, kişinin becerisini geliştirmeye yönelik genel uygulamaya katılmayı; dijital ortamda eğitim için yeni araçlar ve yaklaşımlar öğrenmeyi veya modern dijital araçları kullanmayı; ve sürekli eğitim ve öğretim yoluyla gelişen siber güvenlik tehditleri, gizlilik sorunları ve en iyi uygulamalar hakkında bilgi sahibi olmayı içerir.

- **Dijital vatandaşlık ve etik**

Bu beceri, MEÖ eğitimini gerçekleştirirken düzenlemelere uyarak ve diğer bireylerin ve kuruluşların haklarına saygılı olarak sorumlu dijital vatandaşlık uygulamayı; çevrimiçi ortamlarda etik davranış, saygılı iletişim ve dijital görgü kurallarını öğreterek öğrenciler arasında sorumlu dijital vatandaşlığı teşvik etmeyi; öğrencilerin çevrimiçi bilgilerin güvenilirliğini değerlendirmelerine, dijital riskleri tanımalarına ve çevrimiçi etkinlikleri hakkında bilinçli kararlar almalarına yardımcı olmak için analitik düşünme becerilerini geliştirmeyi; sürece katılan bireylerin ve kuruluşların dijital itibarını korumayı içerir.

Bu beceriler daha önce açıklanan DigCompEdu çerçevesine atıfta bulunabilir, ancak bu çerçevelerde yer alan bireysel yetkinliklerle doğrudan eşleşmeyebilir. Bunun yerine, çerçevedeki yetkinlik alanı tanımlarında MEÖ eğitmenleri ve eğitimcileri için faydalı olan becerilere karşılık gelen unsurlar vardır.

Tablo 1. Önerilen Mesleki Eğitim ve Öğretim eğitmen becerilerinin DigCompEdu yeterlilik alanlarına bağlanması.

Mesleki Eğitim Eğitmeni Becerisi	DigCompEDU Yetkinlik Alanı
Genel siber güvenlik farkındalığı	• Öğrencileri Güçlendirmek • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Veri koruma ve gizlilik	• Dijital Kaynaklar • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Cihaz güvenliği ve yönetimi	• Öğretme ve Öğrenme • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Güvenli dijital iletişim	• Profesyonel Katılım • Değerlendirme
Dijital ayak izi yönetimi	• Dijital Kaynaklar • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Eleştirel düşünme	• Öğretme ve Öğrenme • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Sürekli öğrenme	• Profesyonel Katılım • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması
Dijital vatandaşlık ve etik	• Öğrencileri Güçlendirmek • Öğrencilerin Dijital Yetkinliklerinin Kolaylaştırılması

Bu beceriler, Mesleki Eğitim ve Öğretim eğitmenlerine ve eğitimcilere dijital hijyen konusunda en iyi uygulamalara bağlı kalarak eğitim faaliyetlerine katılma imkânı sağlamaktadır. En iyi uygulamalardan bazılarının ayakları yere basan bir referansı Dijital Hijyen Hile Sayfası olarak mevcuttur [7]. Güvenli dijital yaşamın, dijital dünya hakkında biraz bilgi sahibi olmayı gerektiren 12 ilkesini tanımlamaktadır:

- Çalışma yazılımınızı, antivirüs, güvenlik duvarı vb. güncel tutmak,
- Güvenli parolalar kullanmak, bunları güvenli bir şekilde yönetmek ve çok faktörlü kimlik doğrulama kullanmak,
- Yazılım indirirken dikkatli olmak,
- Varlıklarınızı tehlikeye atmaya yönelik kimlik avı ve diğer şüpheli girişimlerin farkında olmak,
- Dijital ve sosyal ayak izinizi sınırlandırmak,
- Dijital ortamda bilgi ile uğraşırken genel bir "önce güvenlik" zihniyetinin benimsenmesi.

Mesleki eğitim ve öğretimde dijital hijyen becerilerinin edinilmesi ve uygulanması, bilgi alışverişi için güvenli bir ortam sağlanması açısından önemlidir.

Ünite 3- Dijital Hijyenin Mesleki Eğitim ve Öğretim Müfredatına ve Eğitimine Uyarlanması

Dijital Hijyen konuları mesleki eğitimin günlük bir parçası olmalıdır. Mesleki Eğitim ve Öğretim eğitmenleri ve eğitimcileri, eğitim ortamının sağlanmasının bir parçası olarak dijital araçların kullanımını uygulayan eğitimi planlarken ve yönetirken; eğitim materyallerini üretirken ve dağıtırken; akranlar arası ve eğitmen-öğrenci iletişimini organize ederken; eğitim sonuçlarını analiz ederken ve eğitim sürecinin iyileştirilmesi için idari prosedürleri ve planlamayı gerçekleştirirken sağlam dijital hijyen yönergelerini takip etmelidir.

Ayrıca, Mesleki Eğitim ve Öğretim eğitmenleri, eğitimin konusu dijital dünya ile ilgili konular olmasa bile, yürütülen eğitimin etkinliğini artırmak için bu bilgilerin bazılarına ihtiyaç duyulabileceğinin farkında olmalıdır. Eğitmenler, öğrencilerinin olası geçmişlerinin farkında olmalı ve öğrencilerinin dijital hijyenini geliştirecek bazı eğitim uygulamalarının açıklanması ve gösterilmesi için zaman ayırarak ve çaba harcayarak eğitim programını ayarlamalıdır.

Elbette, bazen dijital hijyen ve diğer ilgili konular eğitimin asıl ana konusu olabilir. Bu durumlarda, Mesleki Eğitim ve Öğretim eğitmenleri ve eğitimcileri, dijital hijyenle ilgili yeni bilgiler edinirken ve yeni beceriler kazanırken öğrencilerine rehberlik etmeye devam edebilirler.

Mesleki eğitim ve öğretim eğitmenlerinin bakış açısından dijital hijyen, eğitimin konusundan bağımsız olarak verilen eğitim sırasında güvenli ve üretken dijital faaliyetlerin sürdürülmesi ve sağlanması uygulaması olarak algılanabilir. Mesleki ve eğitim eğitiminin çeşitli yönleri, eğitim sonuçlarını geliştirmek ve eğitime katılan öğrencilerin memnuniyetini artırmak için dijital bir ortamın kullanılmasını gerektirebilir. Eğitmenler, dijital araçların kullanımının eğitim sürecini nasıl etkilediğinin farkında olmalı ve dijital hijyenle ilgili bazı hususları eğitimin kendisine entegre etmeye çalışmalıdır. İşte eğitim sürecinin nasıl iyileştirilebileceğine dair bazı seçenekler:

- **Dijital güvenlikle ilgili konular ve kurs modülleri**

Eğitim içeriği sunarken, belirli bir eğitim faaliyeti başlatmayı önerirken veya öğrencilerden eğitimle ilgili idari bir faaliyet gerçekleştirmelerini isterken, öğrencilere şifre yönetimi, kimlik avı girişimlerini tanıma ve kişisel ve işyeri verilerinin güvenliğini sağlama gibi siber güvenlik temellerini öğreten daha küçük eğitim konuları veya daha kapsamlı modüller şeklinde bazı tavsiyelerde bulunun. Mümkün olduğunda, bu konuları belirli sektörlere, iş kollarına, iş rollerine veya öğrencinin mevcut iş koluyla veya girmeye hazırlandığı beklenen iş kolu veya gelecekteki iş pozisyonuyla ilgili faaliyetlere göre uyarlayın ve bilgileri ilgili ve uygulanabilir hale getirin.

- **Uygulamalı atölye çalışmaları, bireysel ve grup çalışmaları**

Eğitim sırasında uygulamalı atölye çalışmaları veya bireysel ya da grup çalışması ödevleri gibi pratik ödevler verirken, öğrencilerin güvenli ağlar kurma, VPN kullanma, güvenlik yazılımı yükleme ve yönetme ve düzenli güvenlik kontrolleri yapma konusunda pratik yapabilecekleri atölye çalışmaları uygulayın; ya da güvenli bir öğrenme ortamında farkında olmadıkları bazı hataların potansiyel olarak nasıl sorunlara yol açabileceğini deneyimlemelerini sağlayın. Uygulamalı bir yaklaşım ve deneme yanılma fırsatları, pratik uygulama yoluyla teorik bilgilerin pekiştirilmesine yardımcı olur.

- **Etik ve uyumluluk**

Eğitim sırasında, teorik eğitim konularının veya uygulamalı ödevlerin bazı davranışlar üzerinde etkileri varsa, çevrimiçi etik davranış ve dijital eylemlerin yasal sonuçları hakkında tartışmaları dahil edin ve rehberlik sunun. Bu, eğitim konusuyla ilgili veri gizliliği yasaları veya öğrencilerin rolleri ve profesyonel davranışları, etik bilgisayar korsanlığı ve profesyonel bir çevrimiçi varlığı sürdürmenin önemi gibi konuları kapsayabilir.

- **Dijital ayak izi yönetimi**

Çevrimiçi faaliyetlerin kişisel ve mesleki itibar üzerindeki uzun vadeli etkilerini vurgulayarak öğrencileri dijital ayak izlerini yönetme konusunda eğitin. Eğitim, sosyal medyanın nasıl etkin bir şekilde kullanılacağını, dijital içeriğin nasıl yönetileceğini ve çevrimiçi paylaşımların sonuçlarının nasıl anlaşılacağını içerebilir. Öğrencileri, iş için kullanılan dijital araçların da nasıl dijital ayak izi yaratabileceği ve öğrencilerin kendi iş sonuçlarını ve işbirliği sırasında elde edilen başkalarının sonuçlarını nasıl yönetmeleri gerektiği konusunda eğitin.

- **Sürekli öğrenme**

Modern dijital ortamların sürekli değiştiğinin farkında olun. Rollerine ve geldikleri veya katılmayı bekledikleri iş koluna bağlı olarak öğrenciler yeni dijital araçların kullanımıyla ilgili konularda yeni bilgilere ihtiyaç duyabilirler. En son teknolojilerle güncel kalmak ve eğitim konusunu öğrenen öğrencileri etkileyebilecek en yeni tehditlerin farkında olmak önemlidir. Dijital ortamdaki yeni seçenekler hakkında farkındalığın artırılması ve öğrencilere yeni araçların tanıtılması, eğitimin algılanan kalitesinin artmasına ve öğrencilerin bilgi ve becerilerinin gelişmesine yol açabilir. Dijital güvenlik uygulamalarında sürekli öğrenme ve sertifikasyon için fırsatlar aramak, ana eğitim konularından bağımsız olarak müfredatın ayrılmaz bir parçası haline gelebilir.

- **Değerlendirme ve belgelendirme**

Değerlendirmeler eğitimin bir parçasıdır. Eğitimin konusuna ve hedeflerine bağlı olarak değerlendirmeler az ya da çok resmi olabilir ve değerlendirmeyi gerçekleştirmek ve değerlendirme sonuçlarını toplamak ve analiz etmek için dijital araçların kullanımını içerebilir. İyi uygulama, öğrencilerin değerlendirme araçlarının doğru kullanımının farkında olduklarından emin olmaktır. Değerlendirmelerin içeriği, özellikle dijital hijyen alanında kazanılan bilgi ve becerilerin yanı sıra genel konulardaki bilginin test edilmesini de içerebilir. Değerlendirme ve sertifikalar öğrencileri teşvik etmek için kullanılabilir ve sonuçların sunulduğu biçim dijital ortam hakkında

ek düşünce gerektirebilir. Öğrenciler yeni sertifika bilgilerini edinirken ve kullanırken ya da istihdam edilebilirliklerini artırmak için yeni niteliklerini kullanırken yardıma ihtiyaç duyabilirler.

Dijital hijyenle ilgili mesleki eğitimin iyileştirilmesine yönelik seçeneklerden bazılarının daha önce tanımlanan becerilere karşılık geldiğini fark edebilirsiniz. Tüm bu unsurlar mesleki eğitim programlarına dahil edilebilir ve iki farklı perspektiften incelenebilir: eğitimin bir parçası olarak hangi dijital hijyen becerilerinin kullanılması gerektiği ve eğitim sırasında ek dikkat gerektirdiği; ve ana konulara ek olarak eğitim sırasında dijital hijyen bilgi ve becerilerini geliştirmek için ek fırsatların neler olduğu. Bu unsurların ele alınması, eğitimin kalitesini artırabilir ve öğrencilere dijital dünyanın seçeneklerine büyük ölçüde dayanan çalışma ortamlarında ek faydalar sağlayabilir.

Pratik açıdan bakıldığında, Mesleki Eğitim ve Öğretim eğitmenlerinin ve eğitimcilerinin: güvenli öğrenme ortamlarını ve özellikle eğitime tahsis edilmiş araçları tanıtması, eğitim materyallerini ele almak için yönergeler oluşturması, iletişim araçlarını kullanması ve kişisel bilgilerin ve özel bilgilerin korunmasını göz önünde bulundurarak iletişim kurması, genellikle hassas bilgiler içeren eğitim süreci ve sonuçları hakkındaki verileri yönetmesi ve iyi dijital hijyen uygulamalarına uymayı kolaylaştıran genel tavsiyeleri takip etmesi ve sağlaması gerektiği anlamına gelir.

Ünite 4- İyi Uygulama Örneği- Mesleki Eğitim ve Öğretim Kurumları için Dijital Hijyen

Kuruluşun güvenliği ve MEÖ eğitmenlerinin ve eğitime katılan öğrencilerin kullanımı için MEÖ kuruluşunda dijital hijyenin nasıl tanıtılabileceğine dair iyi bir uygulama örneğine bakalım.

Durum açıklaması

Bir mesleki eğitim ve öğretim şirketi, masraflı ve zaman alıcı seyahatlerden kaçınmak ve öğrencilere güvenli fiziksel ortamlarından eğitime katılma kolaylığı sağlamak için öğrencilerine çevrimiçi eğitim vermek istemektedir. Mesleki eğitim ve öğretim şirketi, çevrimiçi eğitim sağlama konusunda daha önce farklı deneyimleri olan ve bu tür bir eğitimi yürütmekle ilgili farklı bilgi ve becerilere sahip olabilecek bir iç ve dış eğitmen kadrosuna sahiptir. Şirketin ayrıca eğitimle ilgili idari faaliyetleri yürüten ve zaman zaman hassas olan ve uyumluluk kuralları ve yönergeleri tarafından ele alınması gereken bilgileri işleyen dahili çalışanları da vardır. Tipik olarak, eğitmenlerin eğitimi yürütmek, eğitim materyallerini paylaşmak ve öğrencilerle iletişim kurmak için Microsoft Teams ortamını kullanmaları beklenirken, dahili destek personeli eğitim öncesinde, sırasında ve sonrasında öğrencileri yönetmek için Microsoft Teams ve e-posta ve eğitim materyallerini yönetmek ve paylaşmak için bir tür belge depolama sistemi kullanacaktır.

MEÖ şirketinin endişe duyduğu konular şunlardır:

- Eğitime katılanlardan herhangi biri tarafından kişisel bilgilerin yanlış kullanımı,
- Şirketin ve dış ortakların özel bilgilerinin dikkatli kullanımı,
- Eğitime erişimin yalnızca hedeflenen kitleyle sınırlandırılması,
- Öğrenciler için zengin bir deneyim sağlamak,
- Piyasada iyi bir eğitim hizmeti sağlayıcısı olarak belirli bir itibar seviyesini korumak.

Bu durumda dijital hijyen sorunlarının nasıl ele alınabileceğini görelim.

Çözüm

Bu tür bir durum karmaşıktır ve dijital hijyenle ilgili çeşitli hususlara dikkat edilmesini gerektirir:

- Microsoft Teams ortamının kurulumunu organize etmek ve eğitim sırasında kullanıcıları yönetmek,
- eğitimi yürüten eğitmenlerin eğitilmesi,
- Öğrencilerin ve eğitmenlerin katılımıyla gerçek eğitim oturumlarının gerçekleştirilmesi,
- Eğitim sırasında kullanılan eğitim materyallerinin taşınması,
- Eğitmen ile öğrenciler ve öğrencilerin kendi aralarındaki iletişimi düzenlemek,
- Eğitim değerlendirmelerinin yapılması ve geri bildirimlerin toplanması.

Bu hususların her biri için iyi uygulamaların daha ayrıntılı bir açıklaması aşağıda yer almaktadır.

Kurulum ve Giriş Yönetimi

Eğitim için Teams: MEÖ kuruluşu çalışanları tarafından günlük iletişim ve bilgi paylaşımı için kullanılan Teams ortamından ayrı bir Teams ortamı kurulmuştur. Eğitim için Microsoft Teams, resmi eğitim kuruluşlarının gereksinimlerini karşılayan MEÖ kuruluşları tarafından kullanılabilir ve eğitimin yürütülmesi için yararlı olan ek özellikler sağlar.

Tek Oturum Açma (SSO): Microsoft Teams'e, Microsoft Teams ortamında kullanılan uygulamalara ve merkezi olarak kullanılan diğer araçlara erişimi kolaylaştırmak için ortak bir kimlik doğrulama platformu (Active Directory gibi) kullanılarak SSO uygulaması gerçekleştirilmiş ve eğitim sırasında MEÖ kuruluşunun onayı ile gerçekleştirilmiştir.

Rol Tabanlı Erişim Kontrolü: Teams içerisinde kullanıcının pozisyonuna göre roller ve izinler atanmıştır. Özellikle, her biri Teams ortamında ayrıcalıkları olan 4 rol atanmıştır: sistem yöneticisi, eğitim yöneticisi (eğitimden önce eğitim oturumlarını düzenleyen ve eğitimden sonra eğitim sonuçlarını analiz eden kişi), eğitmen (eğitimi ve uygulamalı ödevleri yürüten ve eğitim sırasında eğitim materyallerini idare eden kişi) ve öğrenci, özelliklere ve bilgilere uygun erişimi sağlar.

Güvenli Kimlik Doğrulama Uygulamaları: Uygun olduğu durumlarda, hassas bilgilere erişirken daha fazla ayrıcalık atanan kullanıcılar, güvenliği artırmak için çok faktörlü kimlik doğrulama (MFA) ve güçlü parolalar kullanmaları konusunda eğitilmiştir.

Eğiticilerin Eğitimi

Microsoft Teams Eğitim Çalıştayları: Eğitmenler için Microsoft Teams'in nasıl etkili bir şekilde kullanılacağına dair özel atölye çalışmaları planlanmış ve yürütülmüştür ve iç ve dış eğitmenler Teams ortamında güvenli davranış için yönergeler almaya davet edilmiştir. Eğitim, ekiplerin ve kanalların oluşturulması ve yönetilmesi, toplantıların planlanması ve paylaşılan dosyalar ve sohbet gibi işbirliği özelliklerinin kullanılmasını içeriyordu.

Gelişmiş Özellikler Eğitimi: Eğitim deneyimini geliştirebilecek ara odaları, canlı etkinlikler ve üçüncü taraf uygulamaların entegrasyonu gibi gelişmiş özellikler hakkında eğitmenlere ek eğitim verildi ve bu özellikleri eğitim sırasında pratik ödevler olarak uygulama şansı sunuldu.

Sürekli Destek: Tesislere ihtiyaç duyan eğitmenler için internete güvenli bağlantıları olan tam donanımlı fiziksel eğitim odaları sunulmuştur. Kendi tesislerini kullanmak isteyen eğitmenler için eğitimin güvenli bir şekilde yürütülmesine yönelik kılavuzlar sağlanmıştır. Teknik sorunlarla karşılaşılması durumunda eğitmenlere yardımcı olmak üzere özel BT destek personelinin iletişim bilgileri oluşturuldu.

Eğitim Oturumlarının Yürütülmesi

Oturum Planlama: Dahili eğitim yöneticileri ve eğitmenler, oturumları planlamak, hatırlatıcılar ayarlamak ve toplantı davetinde önceden bir gündem sağlamak için bir takvim kullanımı konusunda eğitildi. Yanlış eğitim oturumlarına katılma riskini en aza indirmek için öğrenciler için otomatik davetler ayarlandı.

İnteraktif Özellikler: Tüm eğitmenlere, öğrencilerin ilgisini çekmek ve mümkün olduğunda öğrenmeyi geliştirmek için oturumlar sırasında anketler, sınavlar ve beyaz tahtalar gibi ek Teams özelliklerini kullanmaları tavsiye edilmiştir. Ek araçların ve özelliklerin kullanımına izin verildi ancak eğitmenlere ek bilgi veya pratik ödevler için bunları kullanırken öğrencilere rehberlik etmeleri tavsiye edildi.

Oturumların Kaydedilmesi: Eğitim oturumlarının kaydedilmesi GDPR nedeniyle ciddi şekilde sınırlandırılmış ve yalnızca tüm öğrencilerin açık rızası üzerine gerçekleştirilmiştir. Kayıtlar oluşturulduğunda güvenli bir şekilde saklanmış ve yalnızca eğitim oturumlarına katılanlar tarafından ve yalnızca sınırlı bir süre için erişilebilir olmuştur. Kayıtların genel olarak eğitim içeriğini daha sonra gözden geçirirken öğrenciler için faydalı olduğu düşünülse de, bir MEÖ kuruluşu bunlarla ilgili risklerin farkında olmalıdır.

Ara Odaları: Grup etkinlikleri veya tartışmalar için ara odaları eğitim yöneticisi tarafından kurulmuş, erişim hakları verilmiş ve eğitmenler için uygun eğitimler gerçekleştirilmiştir; böylece eğitmenler eğitimin ilerleyişini yönlendirmek ve izlemek için odalar arasında geçiş yapabilmektedir.

Eğitim Materyallerinin Taşınması

Dosyalar ve Kaynak Paylaşımı: Eğitim sırasında kullanılan tüm eğitim materyalleri güvenli sunucularda saklanmıştır. Eğitim materyallerinin elektronik anahtarları veya eğitim materyallerinin asıl kopyaları özel bir eğitim yöneticisi tarafından kullanıldı. Daha az hassas materyaller için Teams'in ortamı kullanılmıştır.

İşbirliğine Dayalı Düzenleme: Uygulama ödevleri sırasında belgeler veya sunumlar üzerinde gerçek zamanlı olarak işbirliği yaparken eğitmenlere ve öğrencilere Office 365 entegrasyonu gibi resmi yazılımları kullanmaları ve bilgileri aşırı paylaşmamaları tavsiye edilmiştir.

Versiyon Kontrolü: Eğitim materyallerinin bir parçası olan dahili belgelerin versiyon kontrolü MEÖ organizasyonu içinde uygulamaya konmuştur. Tüm eğitmenlere harici eğitim materyalleri için uzman rolünü üstlenmeleri tavsiye edilmiş ve eğitim materyallerinin güncel versiyonlarını tedarik etmedikleri için MEÖ kurumunun itibarına gelebilecek zararı azaltmak amacıyla eğitim materyallerinin, öğrenci kılavuz kitaplarının ve uygulama testlerinin versiyonları için kurum içi eğitim yöneticilerine danışmaları teşvik edilmiştir.

Öğrenciler ve Eğitmenler Arasındaki İletişim

Düzenli Güncellemeler: Ekip sohbeti, duyurular yapmak, güncellemeleri paylaşmak ve eğitim oturumları hakkında geri bildirim sağlamak için kullanıldı.

Özel Kanallar: Belirli eğitim oturumları ve bireysel öğrenci grupları için kanallar oluşturularak odaklanmış tartışmalar ve kaynak paylaşımı kolaylaştırıldı.

Özel Sohbetler: Eğitmen ve öğrenciler arasındaki ek özel sohbetler, yalnızca her iki tarafın da iletişim bilgilerinin merkezi olarak değiş tokuş edilmesini organize eden ekstra iletişimi kabul ettiği durumlarla sınırlıydı.

Değerlendirme ve Geri Bildirim

Geri Bildirim Formları: Eğitim oturumları hakkında geri bildirim toplamak için Microsoft Forms veya MEÖ kuruluşu tarafından dahili olarak geliştirilen özel yazılımların kullanılması zorunlu kılınmıştır. Geri bildirim için kullanılan yazılımın bağlantıları Teams ortamı üzerinden dağıtılmış ve yalnızca hedeflenen kitlenin geri bildirime katılabilmesi sağlanmıştır. Geri bildirim formlarında sağlanan bilgilere erişim, MEÖ kurumunun dahili eğitim yöneticileriyle sınırlandırılmıştır.

Performans Takibi: Görev vermek, iş toplamak ve notlandırılmış geri bildirim sağlamak için Teams'deki görevlendirme özellikleri kullanılmıştır.

Hem teknik ortamın hem de sürece dahil olan prosedürlerin ve rollerin bu şekilde ayarlanması, Microsoft Teams kullanarak kapsamlı, güvenli ve etkileşimli bir eğitim ortamı sağlar ve hem eğitmenlerin hem de öğrencilerin ihtiyaçlarını karşılarken yüksek bir dijital hijyen ve verimlilik standardını korur.

Kaynaklar

1. Vuorikari, R., Kluzer, S. ve Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 TR, Avrupa Birliği Yayın Ofisi, Lüksemburg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. Avrupa e-Yetkinlik Çerçevesi, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [erişim tarihi 15 Nisan 2024].
3. Avrupa Birliği Siber Güvenlik Ajansı (ENISA). European Cybersecurity Skills Framework Role Profiles, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [erişim tarihi 15 Nisan 2024].
4. Punie, Y., editör(ler), Redecker, C., Eğitimcilerin Dijital Yetkinliği için Avrupa Çerçevesi: DigCompEdu, EUR 28775 EN, Avrupa Birliği Yayın Ofisi, Lüksemburg, 2017, ISBN 978-92-79-73718-3 (print),978-92-79-73494-6 (pdf), doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466.
5. Dünya Ekonomik Forumu, "Future of Jobs Report 2023", https://www.weforum.org/publications/the-future-of-jobs-report-2023/
6. Chui, M., Issler, M., Roberts, R., Yee, L. "McKinsey Technology Trends Outlook 2023", https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable
7. Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [erişim tarihi 15 Nisan 2024].

Modül 2 - Mesleki Eğitim ve Öğretim Kurumları için Özelleştirilmiş Dijital Hijyen Müfredatı

Giriş

Dijital hijyen günlük hayatımızda çok daha büyük ve önemli bir rol üstlenmiştir. Dijitalleşmenin hızla büyümesi ve insan faaliyetlerinin tüm alanlarına yayılmasıyla birlikte, dijital ortamlarımızın güvenli olmasını sağlamak için acil bir ihtiyaç ortaya çıkmıştır. Bu bağlamda birincil ve temel önlemlerden biri uygun dijital hijyenin sağlanmasıdır. Kurumların karşı karşıya kaldığı siber tehditlerin giderek arttığı düşünüldüğünde bu özellikle doğrudur. Dijital hijyen öncelikle sağlıklı ve güvenli bir dijital varlığın sürdürülmesine odaklanır ve daha fazla kuruluş faaliyetlerini çevrimiçi ortama taşıdıkça bu konu giderek daha önemli hale gelmiştir. Bu modül, öğrencileri iyi dijital hijyen uygulamaları geliştirmek, değerlendirmek ve sürdürmek için mesleki düzeyde eğitebilecek sağlam bir müfredat sağlamak üzere tasarlanmıştır.

Bu programı almak, öğrencinin kurumsal bir ortamda dijital hijyeni sağlamak için etkili bir şekilde değerlendirmek, sürdürmek ve gerektiğinde müdahale etmek için gerekli temel analitik ve pratik becerileri edinmesini sağlayacaktır. Bu program, piyasada bu alanda becerilere sahip profesyonellere yönelik yüksek talep nedeniyle gerçekten ilgili bir programdır. Bu gelişim programı, bu alandaki en iyi uygulamalarla kıyaslanmıştır. Bu programın odak noktasının yeni başlayanlar ve KOBİ profesyonelleri olması, modüllerin ve yapının seçiminde etkili olmuştur. Programın özü, bu seviyede yeterlilik oluşturmaktır; bu da programın yarı zamanlı veya tam zamanlı olarak almak isteyenler için erişilebilir olacak şekilde tasarlandığı ve yapılandırıldığı anlamına gelmektedir. Program aynı zamanda kısa bir geri dönüş süresi ile uygulamalı ve pratik odaklı olacak şekilde tasarlanmıştır. Bununla birlikte, öğrencilerin kendi hızlarında ilerlemelerini sağlamak için de tasarlanmıştır.

Ünite 1- Müfredata Genel Bakış

Bu el kitabı, Dijital Hijyen alanında Mesleki Eğitim ve Öğretim (VET) programına halihazırda kayıtlı olan veya kayıt yaptırmak üzere olan öğrencilere ve eğitmenlere programın amacı, planlaması, yapısı ve değerlendirmesi ile ilgili bilgi sağlamak amacıyla yazılmıştır. Tüm kuruluşların aynı olmadığının ve aynı düzeyde dijital hijyen becerilerine ihtiyaç duymadığının bilincinde olarak, bu modül ve farklı bölümler

modüler yapıdadır. Bu, belirli alanlarda yetkin olan bireylerin ihtiyaçları geliştikçe diğer modüllere odaklanmalarına veya geçiş yapmalarına olanak tanır. Bu programın nihai hedefi, dijital hijyen konusunda sağlam bir temel oluşturarak hem öğrencileri hem de eğitmenleri siber riskleri etkin bir şekilde yönetme ve azaltma konusunda güçlendirmektir. Bu müfredat aynı zamanda GIAC Security Essentials (GSEC) ve CompTIA Security+ gibi temel düzey profesyonel siber güvenlik sertifikalarının önemli bir kısmını kapsayacak şekilde tasarlanmıştır. Bu nedenle, öğrencilerin bu programa katılmaları için katma değer ve daha fazla teşvik sağlamaktadır.

Modülün Program Amaç ve Hedefleri

Dijital Hijyen modülünün temel hedefleri, katılımcıların aşağıdakileri yapmasını sağlayarak kuruluşların siber güvenlik duruşunu geliştirmek üzere tasarlanmıştır:

- Kurumların karşılaştığı siber güvenlik tehditlerini değerlendirin.
- Temel ağ güvenliğini değerlendirir ve uygular.
- Temel şifreleme protokollerinin nasıl kurulacağını ve sürdürüleceğini bilmek.
- Veri yönetimi ve güvenlik protokollerini değerlendirin ve uygulayın.
- Temel donanım ve yazılım güvenlik protokollerini değerlendirir ve uygular.
- Mobil ortamda güvenliği yönetin.

Öğretim Metodolojisi

Program, teorik eğitim ve pratik uygulamanın bir karışımını kullanır. Öğrencilerin öğrendikleri kavramları gerçek dünya senaryolarında uygulayabilmelerini sağlamak için vaka çalışmaları, uygulamalı laboratuvar oturumları ve etkileşimli atölye çalışmalarından yararlanmaktadır. Bu yaklaşım sadece anlayışı geliştirmekle kalmaz, aynı zamanda mezunların işe hazır olmalarını ve programı tamamladıktan hemen sonra kapsamlı dijital hijyen uygulamalarını hayata geçirebilmelerini sağlar.

Değerlendirme ve Sürekli İyileştirme

Dijital Hijyen programında değerlendirme hem titiz hem de süreklidir ve katılımcıların bilgi ve becerilerini değerlendirmek için çeşitli yöntemler kullanılır. Bunlar arasında kısa sınavlar, uygulamalı sınavlar, proje bazlı değerlendirmeler ve katılımcıların öğrenmelerinin tamamını kapsayan bir bitirme projesi yer almaktadır. Geri bildirim mekanizmaları müfredatın ayrılmaz bir parçasıdır ve katılımcılara ilerlemeleri ve gelişim alanları hakkında zamanında içgörü sağlar. Ayrıca müfredat, siber tehdit istihbaratı ve teknolojik gelişmelerdeki en son gelişmelere uyum sağlamak için düzenli olarak güncellenmekte, böylece güncel siber güvenlik sorunlarının ele alınmasında uygunluk ve etkinlik sağlanmaktadır.

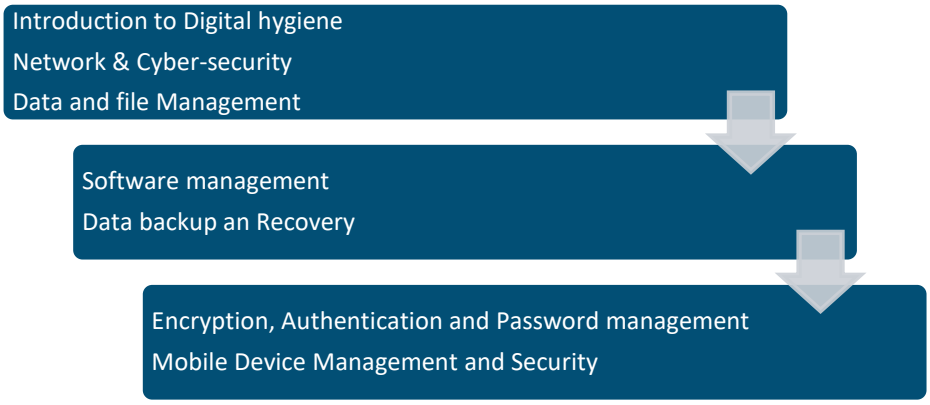
Sonuç

Mesleki Eğitim ve Öğretim Kurumundaki Dijital Hijyen programı, yalnızca temel siber güvenlik bilgi ve becerilerini kazandırmak için değil, aynı zamanda katılımcılar arasında proaktif ve bilinçli bir siber güvenlik kültürü aşılamak için tasarlanmıştır. Programın sonunda katılımcılar sadece mezun olmakla kalmıyor; kurumlarının siber güvenlik savunmalarına önemli ölçüde katkıda bulunabilecek donanıma sahip, güçlendirilmiş dijital vatandaşlar haline geliyorlar. Bu kapsamlı program, dijital çağın dinamik zorluklarının üstesinden gelmeye hazır yeni nesil siber güvenlik profesyonellerinin hazırlanmasında bir mihenk taşıdır.

Ünite 2- Temel Öğrenme Alanları

Müfredata Genel Bakış

Kod	Öğrenme Alanları/Konuları
D21	Dijital Hijyene Giriş
D22	Ağ ve Siber Güvenlik
D23	Veri ve Dosya Yönetimi
D24	Yazılım Yönetimi
D25	Veri Yedekleme ve Kurtarma
D26	Şifreleme, Kimlik Doğrulama ve Parola yönetimi
D27	Mobil Cihaz Yönetimi ve Güvenliği



Dijital Hijyene Giriş

Bu konu, öğrencilere dijital hijyen konusunda kapsamlı bir genel bakış sağlamak üzere tasarlanmıştır. Bu genel bakış, programa bütüncül bir perspektiften bakıldığında hem içeriğe kavramsal bir genel bakış hem de bazı pratik çalışmalar sağlayacaktır. Birincil odak noktası, Dijital hijyenin farklı alanlarını ve farklı konu alanlarının birbiriyle nasıl bağlantılı ve ilişkili olduğunu tanıtmak olacaktır. Dijital hijyenin temel ilke ve uygulamalarına ve farklı bileşenlerin birbirine nasıl uyduğuna dair ön bir genel bakış sağlayacaktır. Bu ünite, diğer bileşen alanlarının üzerine inşa edilebileceği temel bilgi ve anlayışı sağlar.

Bu Konuda Ele Alınan Temel Konular

- Dijital hijyeni anlamak: Dijital hijyeni neyin oluşturduğuna ve günümüz dijital çağında neden kritik olduğuna dair bir keşif.

- Dijital hijyen temelleri: Veri ve sistemlerin bütünlüğünü ve güvenliğini sağlayan temel uygulamalar ve protokoller.
- Dijital hijyenin güvenlik üzerindeki etkileri: Etkili dijital hijyenin çeşitli siber tehditleri nasıl azaltabileceğine ayrıntılı bir bakış.
- Dijital hijyen uygulama temelleri: Kişisel ve kurumsal bağlamlarda dijital hijyen önlemleri almak için pratik adımlar.
- Siber güvenlik uyumluluğu: Siber güvenlikle ilgili temel ulusal ve AB politikalarına, yönetmeliklerine ve uyumluluk gerekliliklerine genel bir bakış

Konu Öğrenme Çıktıları

Bu dersin sonunda öğrenciler şunları yapabileceklerdir:

- Dijital hijyeni tanımlayın ve kritik bileşenlerini anlayın.
- Potansiyel siber tehditleri belirleme ve bu tehditlere karşı korunmada dijital hijyenin rolünü anlama.
- Çeşitli platformlarda ve cihazlarda temel dijital hijyen uygulamalarını hayata geçirin.
- Dijital hijyenin önemini meslektaşlarına ve üstlerine ileterek kurumlarındaki en iyi uygulamaları savunurlar.
- Temel siber güvenlik uyumluluk gerekliliklerini anlayın

Öğretim Yöntemleri

Öğrencilere sağlam bir öğrenme deneyimi sunmak için dersler, interaktif atölye çalışmaları ve vaka çalışmalarının bir karışımı kullanılacaktır. Her oturum, teorik bilgi ile pratik uygulama arasında bir denge kurarak öğrencilerin öğrendiklerini kendi işyerlerinde uygulanabilir stratejilere dönüştürebilmelerini sağlamayı amaçlamaktadır.

Önerilen Literatür

- Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.
    - Bu kitap, siber güvenlik alanına kapsamlı bir giriş sağlar ve özellikle giriş seviyesi siber güvenlik sertifikaları için yararlıdır.
- Paula, D., Cruz, M., (2023), Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - Bu kitap, siber güvenlik sorunlarını ve bunlara karşı nasıl önlem alınacağını anlamak için okunması gereken bir eserdir. Özellikle yeni başlayan KOBİ sahipleri ve çevrimiçi güvenliği anlamak isteyen öğrenciler için önemlidir.
- Singer, P. W., & Friedman, A. (2014). Siber Güvenlik ve Siber Savaş: Herkesin Bilmesi Gerekenler. Oxford Üniversitesi Yayınları.
    - Bu referans, siber güvenlik alanındaki temel kavramlara ve zorluklara erişilebilir bir genel bakış sunarak, siber tehditleri ve koruma mekanizmalarını anlama yolculuğuna başlayan öğrenciler için mükemmel bir kaynaktır.
- Schneier, B. (2015). Veri ve Golyat: Verilerinizi Toplamak ve Dünyanızı Kontrol Etmek için Gizli Savaşlar. W. W. Norton & Company.
    - Bruce Schneier'in kitabı, kişisel verilerin nasıl toplandığı ve kullanıldığı ve sağlam veri yönetimi uygulamalarının önemi hakkında bilgiler sunarak veri gizliliği ve güvenliği ortamını anlamak için çok önemlidir.

Bu kaynaklar, ağ ve siber güvenlik alanında teorik bilgi ve pratik beceriler sağlamak, müfredatı desteklemek ve Mesleki Eğitim ve Öğretim öğrencilerinin dijital hijyen konusundaki eğitim deneyimlerini geliştirmek için seçilmiştir.

Ağ ve Siber Güvenlik

Bu konu, öğrencilere ağ tehditlerini tanımlamak, değerlendirmek ve etkisiz hale getirmek için gerekli becerileri sağlamaya odaklanmıştır. Mevcut çalışma ortamlarında kuruluşların karşılaştığı en önemli zorluklardan biri ağ güvenliğini sağlamaktır. Çoğu ağ internete bağlı olduğundan, genellikle ağa yetkisiz bir şekilde erişmek için ağ güvenlik açıklarından yararlanmaya çalışabilecek kötü niyetli aktörlere maruz kalırlar. Bunu başarmak için öğrenci temel ağ kavramları, ortak protokoller, bağlantı noktaları, LAN, WAN ve bulut sistemleri konusunda bilgilendirilecektir.

Bu Konuda Ele Alınan Temel Konular

- Siber güvenliğe giriş
- Güvenlik açığı analizi
- Tehdit ve risk değerlendirmesi
- Ağ güvenliği protokolleri - Güvenlik duvarları, antivirüs.
- Yaygın siber güvenlik saldırıları
- Yaygın Siber Güvenlik araçları
- Siber güvenlikte etik

Öğrenme Çıktıları

- Temel Ağ Kavramlarını Tanımlama: Öğrenciler, LAN, WAN ve bulut sistemleri dahil olmak üzere ağların temel yönlerini tanımlayabilecek ve kurumsal altyapıdaki rollerini anlayabileceklerdir.
- Ağ Güvenlik Açıklarını Değerlendirme: Katılımcılar, potansiyel güvenlik zayıflıklarını belirlemek için çeşitli ağ sistemleri üzerinde güvenlik açığı analizleri gerçekleştirme becerisi kazanacaklardır.
- Güvenlik Önlemlerini Uygulamak: Öğrenciler, siber tehditlere karşı korunmak için güvenlik duvarları ve antivirüs sistemleri gibi ağ güvenlik protokollerini kurma ve yönetme konusunda yetkin olacaklardır.
- Tehdit ve Risk Değerlendirmeleri Yapmak: Öğrencileri, ağ sistemlerine yönelik siber güvenlik tehditleriyle ilişkili riskleri değerlendirme ve önceliklendirme becerisiyle donatmak.
- Etik Sonuçları Anlamak: Öğrenciler, veri ve sistemleri yetkisiz erişimden korumanın sorumluluklarını anlayarak siber güvenlikteki etik hususları keşfedeceklerdir.

Öğretim Yöntemleri

- İnteraktif Dersler: Temel ve gelişmiş ağ kavramlarını, güvenlik protokollerini ve siber güvenlikteki etik konuları tanıtmaya odaklanmıştır.
- Uygulamalı Laboratuvarlar: Öğrencilerin güvenlik önlemlerini ve araçlarını uygulamak için gerçek ve simüle edilmiş ağ ortamlarını kullanabilecekleri bilgisayar laboratuvarlarında uygulamalı oturumlar.
- Vaka Çalışması Analizi: Tehdit mekanizmalarını ve etkili karşı önlemleri anlamak için gerçek dünyadaki siber güvenlik olaylarının tartışılması ve analizi.

- Grup Projeleri: Öğrenci takımları, varsayımsal bir ağ kurulumunu güvenlik açıkları açısından değerlendirecek ve kapsamlı bir güvenlik stratejisi önerecektir.
- Konuk Konuşmacı Oturumları: Siber güvenlik uzmanları, mevcut zorlukları ve gelişmekte olan teknolojileri vurgulayarak görüşlerini ve deneyimlerini paylaşmaya davet edilmektedir.

Tavsiye edilen literatür

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7. baskı). Cengage Learning.
    - Bu kılavuz, siber güvenlik yolculuğuna başlayan öğrenciler için uygun olan, ağ güvenliğindeki temel konuları geniş bir yelpazede ele almaktadır.
- Marsh, N., (2023), Siber Güvenlik: Ağ Güvenliği En İyi Uygulamaları için Yağsız Rehber (Yağsız Teknoloji Rehberleri). Bu kitap, siber tehditler ve kritik ağ güvenliği konuları hakkında kapsamlı bir bakış açısı sunmaktadır.
- Whitman, M. E., & Mattord, H. J. (2018). *Bilgi Güvenliği İlkeleri* (6. baskı). Cengage Learning.
    - Güvenlik açığı analizi, tehdit ve risk değerlendirmesi hakkında ayrıntılı tartışmalar da dahil olmak üzere bilgi güvenliği ilkelerine derinlemesine bir bakış sağlayan kapsamlı bir kaynak.
- Stallings, W. (2017). Ağ Güvenliği Temelleri: Uygulamalar ve Standartlar (6. baskı). Pearson. Stallings'in metni, ağ güvenliği protokollerini ve standartlarını kapsamlı bir şekilde ele almaktadır ve ağ güvenliğinin teknik yönlerini ayrıntılı bir şekilde anlamaya ihtiyaç duyan öğrenciler için idealdir.
- Bilgisayar ve İnternet Güvenliği: Uygulamalı Yaklaşım 3. Baskı, Wenliang Du

Bu akademik kaynaklar, ana hatlarıyla belirtilen öğrenme çıktıları ve öğretim stratejileriyle uyumlu olacak şekilde, ağ ortamlarını yönetme ve güvence altına alma konusunda hem teorik çerçeveler hem de pratik bilgiler sağlayarak müfredatı destekleyecektir.

Veri ve Dosya Yönetimi

Daha önce de belirtildiği gibi veri, kuruluşların sahip olduğu en değerli varlıklardan biridir. Sonuç olarak, bu varlığın yönetimi kuruluş içinde giderek daha hayati bir rol üstlenmiştir. Bu özellikle siber ortamda güvenlik endişelerinin artması nedeniyle önemlidir. Doğru veri yönetimi, özellikle hassas bilgilerin yakalanması, düzenlenmesi ve yayılmasında etkili siber güvenlik için çok önemli hale gelmiştir. Veri yönetimi, verilerin yönetimi ve korunmasında uygulanan ilke ve uygulamaları ifade eder. Siber güvenlik bağlamında veri yönetimi, verilerin yetkili erişim değişikliklerinden ve iletiminden korunması ile de ilgilidir. Büyük hacimlerde verinin toplandığı, analiz edildiği ve yayıldığı mevcut ortamda, güvenlik yönetimine ilişkin hususlar önem kazanmıştır. Bu nedenle, veri yönetimi konusunda yetkin profesyonellere duyulan ihtiyaç artmıştır.

Bu Konuda Ele Alınan Temel Konular

- Veri yönetişimi
- Veri sınıflandırması
- Veri yönetiminde şifreleme
- Veri İzleme ve Denetim
- Veri yedekleme ve kurtarma
- Veri bütünlüğü ve gizliliği
- Erişim kontrolleri ve kimlik doğrulama

Öğrenme Çıktıları

- Veri Yönetişimini Anlamak: Öğrenciler veri yönetişiminin temel kavramlarını ve kurumsal bağlamdaki rolünü kavrayacaklardır.
- Verileri Sınıflandırma: Öğrenciler, verileri hassasiyet ve öneme göre sınıflandırabilecek ve farklı veri türlerine uygun güvenlik önlemlerini uygulayabilecektir.
- Veri Şifrelemeyi Uygulama: Öğrenciler, depolama ve iletim sırasında veri bütünlüğünü ve gizliliğini korumak için şifreleme tekniklerini anlayacak ve uygulayacaklardır.
- Veri Denetimleri Gerçekleştirin: Öğrencileri, güvenlik politikaları ve yönetmelikleriyle uyumluluğu sağlamak için düzenli veri izleme ve denetimleri gerçekleştirme becerileriyle donatın.
- Veri Kurtarmayı Yönetme: Öğrenciler, veri kaybı veya sistem arızaları durumunda veri kullanılabilirliğini ve sürekliliğini sağlamak için veri yedekleme ve kurtarma stratejilerini öğreneceklerdir.
- Veri Bütünlüğünü ve Gizliliğini Sağlama: Öğrenciler, kullanıcı verilerini yetkisiz erişime karşı korumak için veri bütünlüğünü koruma ve gizlilik ayarlarını yönetme yöntemlerini anlayacaklardır.
- Erişim Kontrollerini Uygulayın: Öğrenciler, veri erişimini korumak için sağlam erişim kontrolleri ve kimlik doğrulama yöntemleri uygulayabileceklerdir.

Önerilen Literatür

- Ladley J., (2019), Veri Yönetişimi: How to Design, Deploy, and Sustain an Effective Data Governance Program 2. Baskı. Bu kitap, veri yönetişimi ve güvenliğine ilişkin kapsamlı bir bakış açısı sunmaktadır.
- Talabis, M., & Martin, J. (2015). Bilgi Güvenliği Risk Değerlendirme Araç Seti: Veri Toplama ve Veri Analizi Yoluyla Pratik Değerlendirmeler. Syngress.
    - Bu kitap, veri yönetimi ile ilişkili olanlar da dahil olmak üzere bilgi güvenliği risklerini değerlendirmek için pratik araçlar ve teknikler sunmaktadır.
- Bertino, E., & Sandhu, R. (2017). Veri Gizliliği ve Güvenliği. Springer.
    - Veri gizliliği ve güvenliği tekniklerine kapsamlı bir genel bakış sunan bu metin, çeşitli ortamlarda hassas verilerin korunmasının karmaşıklığını anlamak için çok önemlidir.
- Swanson, M., & Guttman, B. (2016). Bilgi Teknolojisi Sistemlerinin Güvenliği için Genel Olarak Kabul Edilen İlkeler ve Uygulamalar. Ulusal Standartlar ve Teknoloji Enstitüsü.
    - Bu hükümet yayını, veri yönetimi ve güvenlik kontrollerine ilişkin ayrıntılı bölümler de dahil olmak üzere BT sistemlerinin güvenliğini sağlamaya yönelik kılavuz ilkeler ve en iyi uygulamaları sunmaktadır.

Bu akademik kaynaklar, teorik bilgi ve pratik uygulama örnekleri sağlayarak eğitim çerçevesini geliştirecek ve öğrencilerin kurumsal verileri etkin bir şekilde yönetme ve güvence altına alma konusunda yetkin olmalarını sağlayacaktır.

Yazılım Yönetimi

Yazılım yönetimi, siber güvenliğin çok önemli bir unsurudur. Yazılım yönetimi, yazılımın yaşam döngüsü boyunca planlanması, dağıtılması, izlenmesi ve sürdürülmesine ilişkin sistematik süreci içerir. Sürüm kontrolü, yama yönetimi, lisanslama ve güvenlik güncellemeleri gibi görevleri kapsar. Etkili yazılım yönetimi, riskleri ve güvenlik açıklarını en aza indirirken optimum performans, güvenlik ve uyumluluk sağlar. Modern kuruluşlar yazılım güvenliği konusunda zayıf parola politikaları, güvensiz API yamalanmamış güvenlik açıkları, kimlik avı ve veri ihlalleri gibi çeşitli zorluklarla karşı karşıyadır. Bu nedenle, kuruluşun yazılımını etkin bir şekilde

yönetmek ve yazılım güvenliği ihlallerini önlemek için eğitilmiş personele sahip olmaları zorunludur. Bu modül, öğrenciye kuruluşun yazılımının nasıl etkin bir şekilde yönetileceği ve güvenlik ihlali riskinin nasıl en aza indirileceği konusunda temel uygulamalı bilgi sağlayacaktır.

Bu Konuda Ele Alınan Temel Konular

- Uygulama Güvenliği
- Yazılım testi ve denetimi
- Kullanıcı erişimini ve ayrıcalıklarını yönetme
- Düzenli Güncelleme protokollerinin uygulanması
- Uç nokta güvenlik önlemleri

Öğrenme Çıktıları

- Uygulama Güvenliğinde Uzmanlaşın: Öğrenciler, yaygın güvenlik açıkları ve azaltma stratejileri de dahil olmak üzere tasarımdan dağıtıma kadar uygulamaların güvenliğini sağlamanın temellerini anlayacaklardır.
- Yazılım Testi ve Denetimi Yapma: Katılımcılar, güvenlik sorunlarını belirlemek ve çözmek için çeşitli yazılım testi ve denetimi yöntemlerinde yeterlilik kazanacaklardır.
- Kullanıcı Erişimini Yönetme: Öğrenciler, kritik yazılım kaynaklarına yalnızca yetkili kullanıcıların erişebilmesini sağlamak için kullanıcı erişimini ve ayrıcalıklarını etkin bir şekilde yönetmeyi öğreneceklerdir.
- Güncelleme Protokollerini Uygulamak: Öğrencileri, güvenlik açıklarını azaltmak için düzenli yazılım güncelleme protokolleri oluşturma ve sürdürme bilgisiyle donatın.
- Uç Nokta Güvenliğini Geliştirin: Öğrenciler, kurumsal altyapıyı kötü amaçlı yazılım ve fidye yazılımı gibi tehditlerden korumak için uç nokta güvenlik önlemlerini anlayacaklardır.

Önerilen Literatür

- Du, W., (2022), Bilgisayar Güvenliği: Uygulamalı bir yaklaşım, 3rd baskı. Bu kitap yazılım yönetimi, güvenlik açıkları ve azaltma faaliyetlerini incelemektedir.
- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Yazılım Güvenliği Mühendisliği: Proje Yöneticileri için Bir Kılavuz. Addison-Wesley Professional.
    - Bu kitap, güvenlik uygulamalarını yazılım geliştirmeye entegre etmek için kapsamlı bir rehber sunarak uygulama güvenliği ve yaşam döngüsü yönetimini anlamak için gerekli hale getiriyor.
- Anton, A. I., & Earp, J. B. (2004). Bir Paydaş Tanımlama ve Belirginlik Teorisi: Kimin ve Neyin Gerçekten Önemli Olduğu İlkesinin Tanımlanması. Academy of Management Review.
    - Etkili yazılım yönetimi için çok önemli olan kilit paydaşları ve ihtiyaçlarını belirleyerek kullanıcı erişimini ve ayrıcalıklarını yönetme konusunda içgörüler sağlar.
- Lindqvist, U., & Neumann, P. G. (2017). Siber Güvenliğin Geleceği: Zorluklar ve Fırsatlar. IEEE Güvenlik ve Gizlilik.
    - Bu makalede, sürekli yazılım güncellemelerinin ve uç nokta güvenlik önlemlerinin önemi de dahil olmak üzere siber güvenlik alanında gelecekte karşılaşılacak zorluklar ve fırsatlar ele alınmaktadır.

Bu kaynaklar, yazılım yönetimi konusunda sağlam bir teorik temel ve pratik bilgiler sağlayarak müfredatı destekleyecek ve öğrencilerin modern kurumsal ortamlardaki yazılım güvenliği zorluklarının üstesinden gelebilecek donanıma sahip olmalarını sağlayacaktır

Veri Yedekleme ve Kurtarma

Bu modül, öğrencileri Yedekleme ve Kurtarma süreci ve bunun nasıl uygulanabileceği konusunda kapsamlı bir anlayışla donatmak için tasarlanmıştır. Tüm modern kuruluşlar uygun yedekleme ve kurtarma politikalarına, protokollerine ve sistemlerine sahip olmalıdır. Günümüz kuruluşlarının çoğu veri odaklıdır ve dolayısıyla veri ve bilgi kaynaklarının yönetimine büyük önem vermektedir. Prensip olarak, çoğu kuruluş, özellikle de KOBİ'ler verilerini merkezi bir yerel veya bulut veritabanında depolar. Bulut tabanlı sistemler, çok gelişmiş yönetim kontrolleriyle daha gelişmiş ve güvenli hale gelmiştir ve bu da onları fiziksel depolama sistemlerinin geleneksel tahribat sorunlarına daha az duyarlı hale getirmektedir. Ancak yine de insan hatasına, yanlış yapılandırmaya ve veri ihlallerine açıktırlar, bu nedenle bu tür sistemleri denetleyen BT personelinin ilgili teknolojiler, protokoller ve süreçler hakkında bilgi sahibi olması önemlidir. Bu modül, öğrenciye bu bilgiyi sağlamak üzere tasarlanmıştır.

Bu Konuda Ele Alınan Temel Konular

- Dosya Yönetimi
- Yedekleme ve Kurtarma Protokolleri
- Yedekleme türleri
- Yedekleme hizmetleri ve cihazları

Öğrenme Çıktıları

- Dosya Yönetimini Anlayın: Öğrenciler, yedekleme amacıyla verileri düzenlemek için çok önemli olan etkili dosya yönetimi ilkelerini öğreneceklerdir.
- Yedekleme ve Kurtarma Protokollerinde Uzmanlaşma: Katılımcılar farklı yedekleme ve kurtarma protokollerini ve bunların çeşitli senaryolarda nasıl etkili bir şekilde uygulanacağını anlayacaklardır.
- Yedekleme Türlerini Tanımlama: Öğrenciler farklı yedekleme türlerini (tam, artımlı, diferansiyel) ayırt edebilecek ve belirli durumlar için hangisinin en uygun olduğuna karar verebileceklerdir.
- Yedekleme Hizmetlerini ve Cihazlarını Kullanma: Öğrencileri, bulut tabanlı ve yerel yedekleme çözümleri de dahil olmak üzere çeşitli yedekleme hizmetleri ve cihazları ve bunların güvenli bir şekilde nasıl uygulanacağı hakkında bilgi ile donatın.
- Veri Kaybı Risklerini Azaltma: Öğrenciler, veri ihlalleri veya felaketler durumunda kesinti süresini ve veri kaybını en aza indirmek için bir veri kurtarma stratejisinin nasıl planlanacağını ve yürütüleceğini anlayacaklardır.

Önerilen Literatür

- Preston, W., (2021), Modern Veri Koruma: Tüm Modern İş Yüklerinin Kurtarılabilirliğini Sağlamak. Bu kitap, modern veri koruma ve bunun genel donanım ve yazılım güvenliğine nasıl entegre edildiği ile ilgilidir.
- Veri Yedekleme ve Kurtarma Eksiksiz Bir Kılavuz - 2023 Baskısı
- Toigo, J. W. (2009). Felaket Kurtarma Planlaması: Düşünülemez Olana Hazırlanmak (3. baskı). Prentice Hall.
    - Felaket kurtarmanın kritik bir bileşeni olan yedekleme stratejileri hakkında ayrıntılı tartışmalar da dahil olmak üzere felaket kurtarma planlaması hakkında kapsamlı bilgiler sunar.
- Duffy, D. (2014). Bulut Bilişim: Bulut Bilişimin Benimsenmesi için Stratejiler. Sadık Kalem Yayıncılık.
    - Bulut tabanlı yedekleme hizmetlerine ve bunlarla ilişkili güvenlik hususlarına odaklanarak bulut bilişimin benimsenmesini tartışır.

Bu akademik kaynaklar, öğrencilere modern kurumsal ortamlarda potansiyel veri kaybını en aza indirmek için gerekli olan veri yedekleme ve kurtarma stratejilerini yönetme ve uygulama konusunda hem temel bir anlayış hem de pratik beceriler sağlayarak müfredatı destekleyecektir.

Kriptografi, Kimlik Doğrulama ve Parola Yönetimi

Veri ve bilgi en önemli kurumsal varlıklardan biri haline gelmiştir ve çoğu durumda şirket değerlemesinin arkasındaki temel belirleyicidir. Bu tür varlıkların hayati niteliği, onlara azami özen gösterilmesini zorunlu kılmaktadır. Veri ve bilgi varlıklarını korumanın temel araçlarından biri kriptografidir. Kriptografi, hassas veri ve bilgilerin korunması ve güvenli iletişim için gerekli olduğundan siber güvenliğin merkezinde yer alır. Sağlam kimlik doğrulama protokolleri ve parola yönetimi sağlar. Kriptografi, kurumsal veri ve bilgilerin uygun personele gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan kimlik doğrulama sistemlerinin düzgün bir şekilde uygulanmasını sağlar.

Bu Konuda Ele Alınan Temel Konular

- Kriptografi temelleri
- Uçtan uca şifreleme
- Şifreleme standartları
- Çok faktörlü kimlik doğrulama
- Anahtar yönetimi
- İşletmeniz için en iyi standartları seçme
- Şifreleme teknolojilerinin uygulanmasında en iyi uygulamalar

Öğrenme Çıktıları

- Kriptografi Temellerini Anlayın: Öğrenciler, tarihçesi, amacı ve anahtar mekanizmaları dahil olmak üzere kriptografinin temel ilkelerini öğreneceklerdir.
- Uçtan Uca Şifrelemeyi Uygulama: Katılımcılar, iletişimi güvence altına almak için uçtan uca şifreleme kurma ve yönetme becerileri kazanacaklardır.
- Şifreleme Standartlarını Uygulama: Öğrenciler çeşitli şifreleme standartlarına aşina olacak ve bunları kurumsal ihtiyaçlara göre nasıl uygulayacaklarını öğreneceklerdir.
- Çok Faktörlü Kimlik Doğrulamayı Kullanma: Öğrencileri, güvenliği artırmak için çok faktörlü kimlik doğrulama sistemlerini uygulama ve yönetme becerisiyle donatın.
- Kriptografik Anahtarları Yönetme: Öğrenciler, kriptografik anahtarların güvenliğini ve bütünlüğünü sağlamak için anahtar yönetimi süreçlerini ve en iyi uygulamaları anlayacaklardır.
- Şifreleme Teknolojilerini Seçme ve Uygulama: Öğrenciler, işletmeleri için uygun şifreleme teknolojilerini nasıl seçeceklerini ve verileri etkili bir şekilde korumak için uygulamaya yönelik en iyi uygulamaları öğreneceklerdir.

Önerilen Literatür

- Stallings, W. (2017). Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulama (7. baskı). Pearson.
    - Bu ders kitabı, şifreleme teknolojileri ve kimlik doğrulama protokollerinin ayrıntılı kapsamı dahil olmak üzere kriptografi ve ağ güvenliği alanına kapsamlı bir giriş sağlar.
- Katz, J., & Lindell, Y. (2014). Modern Kriptografiye Giriş (2. baskı). CRC Press.

    - Titiz güvenlik kanıtlarına ve pratik uygulamalara odaklanarak modern kriptografik tekniklerin derinlemesine bir incelemesini sunar.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Kriptografi Mühendisliği: Tasarım İlkeleri ve Pratik Uygulamalar. Wiley.
    - Bu kitap, güvenlik açıklarını önlemek için doğru uygulamanın önemini vurgulayarak kriptografik sistemlerin tasarımını ve uygulanmasını tartışmaktadır.

Bu kaynaklar, kriptografi, kimlik doğrulama ve şifre yönetimi konularında teorik bir altyapı ve pratik beceriler sağlamak üzere seçilmiş olup, müfredatın öğrencileri kurumsal verilerin etkin bir şekilde güvence altına alınması için gerekli bilgilerle donatma hedefini desteklemektedir.

Mobil Cihaz Yönetimi ve Güvenliği

Kuruluşlar mobil cihazları giderek daha fazla ana çalışma platformu ve iletişim aracı olarak kullanmaktadır. Bu durum özellikle çevik ve her zaman ulaşılabilir olmanın başarı için önemli bir kriter haline geldiği startup ve KOBİ'ler için geçerlidir. Mobil teknoloji, en gelişmiş akıllı telefonların dizüstü ve masaüstü bilgisayarlar kadar güçlü ve çok yönlü olmasını sağlayacak kadar ilerlemiş olsa da, bu tür cihazların kablosuz yapısı, onları yetkisiz erişim elde etmek isteyen kötü niyetli aktörlere karşı hassas hale getirmektedir. Bu modül, bu cihazların ve ilgili platformlarının güvenlik açıkları ve bu tür risklerin nasıl en aza indirilebileceği hakkında fikir vermek üzere tasarlanmıştır.

Bu Konuda Ele Alınan Temel Konular

- Mobil cihazlara yönelik tehditlerin anlaşılması
- Mobil uygulamalar için risklerin değerlendirilmesi
- Süreçler arası iletişim güvenlik duvarları
- Mobil güvenlik teknolojileri
- Mobil veri erişim kontrolleri ve risk yönetimi

Öğrenme Çıktıları

- Mobil Cihazlara Yönelik Tehditleri Tanımlama: Öğrenciler, mobil platformları hedef alan çeşitli tehditleri tanımayı ve potansiyel etkilerini anlamayı öğreneceklerdir.
- Mobil Uygulamalar için Riskleri Değerlendirme: Katılımcılar, güvenlik açıklarına odaklanarak mobil uygulamalarla ilişkili riskleri değerlendirme becerisi kazanacaklardır.
- Mobil Güvenlik Teknolojilerini Uygulamak: Öğrenciler, özellikle mobil cihazlar için tasarlanmış güvenlik teknolojilerini uygulayabilecek ve yönetebileceklerdir.
- İşlemler Arası İletişim Güvenlik Duvarlarını Yönetme: Öğrencileri, mobil cihazlarda işlemler arası iletişimi kontrol eden güvenlik duvarlarını yapılandırma ve yönetme bilgisiyle donatın.
- Mobil Veri Erişim Kontrollerini Uygulama: Öğrenciler, mobil cihazlardaki hassas bilgileri güvence altına almak için veri erişim kontrollerini nasıl oluşturacaklarını ve uygulayacaklarını öğreneceklerdir.

Önerilen Literatür

- Doherty, J., (2021), Kablosuz ve Mobil Cihaz Güvenliği 2. Baskı. Bu kitap, mobil cihazların kurumun iletişim ortamına hızla entegre edilmesinin sonuçlarını, buna bağlı güvenlik endişelerini ve bunların nasıl azaltılabileceğini incelemektedir.

- Russell, B., Van Duren, Drew., (2018), Practical Internet of Things Security - Second Edition: İnternete bağlı Ekosistem için bir güvenlik çerçevesi tasarlayın
- Zdziarski, J. A. (2015). iOS Uygulamalarını Hacklemek ve Güvenliğini Sağlamak: Verilerin Çalınması, Yazılımların Ele Geçirilmesi ve Bunların Nasıl Önleneceği. O'Reilly Media, Inc.
    - Bu kitap, iOS'un güvenlik mimarisine derinlemesine bir bakış sunmakta, yaygın güvenlik açıklarını tartışmakta ve iOS uygulamalarının güvenliğini sağlamak için stratejiler sunmaktadır.
- Fried, S. (2011). Mobil Cihaz Güvenliği: Hareketli Bir Dünyada Bilgilerinizi Güvence Altına Almak İçin Kapsamlı Bir Kılavuz. CyberAge Books.
    - Bu kılavuz, hem kişisel hem de profesyonel bağlamlarda giderek daha fazla kullanılan mobil cihazların sunduğu özel güvenlik zorluklarını anlamaya ihtiyaç duyan öğrenciler ve uygulayıcılar için gereklidir.

Bu kaynaklar, mobil cihazları etkin bir şekilde yönetmek ve güvence altına almak için gereken temel bilgileri ve özel becerileri sağlayarak müfredatı destekleyecek ve öğrencilerin modern kurumsal bağlamlarda mobil güvenlik zorluklarını ele almak için iyi hazırlanmış olmalarını sağlayacaktır.

Ünite 3- Mesleki Eğitim ve Öğretim Kurumları için Dijital Hijyen Değerlendirme ve Geri Bildirim Mekanizmaları

Giriş

Değerlendirme ve geri bildirim, eğitim sürecinin çok önemli bileşenleridir ve hem eğitmenlere hem de öğrencilere öğretme ve öğrenmenin etkililiğine ilişkin temel bilgiler sağlar. Dijital Hijyen müfredatı bağlamında, sağlam değerlendirme ve geri bildirim mekanizmaları özellikle kritik öneme sahiptir. Bu mekanizmalar, öğretilen bilgi ve becerilerin sadece anlaşılmasını ve akılda tutulmasını değil, aynı zamanda dijital güvenlik risklerinin yaygın olduğu gerçek dünya senaryolarında da uygulanabilir olmasını sağlar.

Bu ünite, Dijital Hijyen programı boyunca öğrenci performansını değerlendirmeye ve yapıcı geri bildirim sağlamaya yönelik strateji ve metodolojilerin ana hatlarını çizmek üzere tasarlanmıştır. Bu, teorik bilgi değerlendirmeleri ve pratik, uygulamalı değerlendirmelerin bir kombinasyonunu içerir.

Değerlendirme Stratejileri

Biçimlendirici Değerlendirmeler

- **Kısa Sınavlar ve Kısa Testler:** Temel kavramların anlaşılmasını değerlendirmek ve anında geri bildirim sağlamak için her modül boyunca sık sık kısa sınavlar ve kısa testler yapılacaktır. Bu, öğrenmeyi pekiştirmeye ve öğrencilerin ek desteğe ihtiyaç duyabilecekleri alanları belirlemeye yardımcı olur.
- **Pratik Ödevler:** Öğrencilere, bir güvenlik duvarının yapılandırılması, bir veri kurtarma planının tasarlanması veya şifreleme protokollerinin uygulanması gibi teorik bilgileri pratik senaryolara uygulamalarını gerektiren ödevler verilecektir.
- **Akran Değerlendirmeleri:** Bu, öğrencilerin birbirlerinin ödevlerini veya projelerini değerlendirmesini içerir. Öğrenciler en iyi uygulamalara dayalı siber güvenlik çözümlerini eleştirmeyi öğrendiklerinden, akran değerlendirmeleri eleştirel düşünme ve analitik becerilerin geliştirilmesine yardımcı olabilir.

Özetleyici Değerlendirmeler

- **Final Sınavları:** Her modülün sonunda yapılacak kapsamlı sınavlar, öğrencileri kurs boyunca ele alınan daha geniş bir konu yelpazesinde test edecektir. Bu sınavlar, öğrencilerin teorik ve pratik anlayışlarını değerlendirmek için hem çoktan seçmeli soruları hem de kompozisyon tipi soruları içerecektir.
- **Bitirme Projeleri:** Programın sonunda öğrenciler, varsayımsal kuruluşlar için kapsamlı dijital hijyen stratejileri oluşturmayı veya yönetmeyi içeren bir bitirme projesi üstlenecektir. Bu proje, yenilikçilik, uygulanabilirlik ve siber güvenlik ilkelerine bağlılık gibi çeşitli kriterlere göre değerlendirilecektir.

Sürekli Değerlendirme

- **Portföy İncelemeleri:** Öğrenciler, program boyunca çalışmalarını ve başarılarını içeren bir portföy tutacaklardır. Bu portfolyolar, ilerlemeyi değerlendirmek ve kişiselleştirilmiş geri bildirim sağlamak için eğitmenler tarafından periyodik olarak gözden geçirilecektir.
- **Öz Değerlendirmeler:** Öğrencileri öz değerlendirme yapmaya teşvik etmek, öğrenmeleri için daha fazla sorumluluk almalarını sağlayabilir. Öğrencilerin anlayış ve becerilerini değerlendirmelerine yardımcı olmak için öz değerlendirme araçları ve kontrol listeleri sağlanacaktır.

Geri Bildirim Mekanizmaları

- **Eğitmen Geri Bildirimi:** Geri bildirim, öğrencilerin çalışmalarının güçlü ve zayıf yönlerine odaklanarak tüm değerlendirmeler için sistematik olarak sağlanacaktır. Bu geri bildirim zamanında, spesifik ve yapıcı olacak, öğrencileri öğrenmeleri üzerinde düşünmeye ve gelişim alanlarını belirlemeye teşvik etmeyi amaçlayacaktır.
- **Akran Geri Bildirimi:** Grup projelerinde ve akran değerlendirmelerinde, öğrenciler birbirlerine geri bildirim sağlamaya teşvik edilecektir. Bu, yapıcı ve belirli kriterlere odaklanmış olmasını sağlamak için yapılandırılacaktır.
- **Otomatik Geri Bildirim:** Belirli değerlendirme türleri, özellikle de kısa sınavlar ve bazı pratik alıştırmalar için otomatik geri bildirim sistemleri kullanılacaktır. Bu sistemler anında sonuç ve içgörü sağlayarak hızlı düzeltme yapılmasına olanak tanıyabilir.
- **Geri Bildirim Döngüleri:** Müfredat içinde öğrencilerin geribildirim üzerinde düşünebilecekleri, çalışmalarını gözden geçirebilecekleri ve daha fazla inceleme için yeniden gönderebilecekleri geribildirim döngüleri oluşturmak, büyüme zihniyetini ve sürekli gelişimi teşvik eder.

Geri Bildirimin Müfredat Gelişimine Uygulanması

Bu çeşitli mekanizmalardan alınan geri bildirimler sadece öğrencilerin yararına değildir. Aynı zamanda müfredat geliştirmede de önemli bir rol oynar:

- **Müfredat Ayarlamaları:** Öğrenci performans verilerinin ve geri bildirimlerin düzenli olarak gözden geçirilmesi, müfredatın ayarlama veya iyileştirme gerektirebilecek alanlarının belirlenmesine yardımcı olacaktır.
- **Eğitmen Gelişimi:** Öğrencilerden alınan geri bildirimler, eğitmenlerin mesleki gelişim ihtiyaçlarına da rehberlik ederek daha fazla desteğe veya eğitime ihtiyaç duyabilecekleri alanları gösterebilir.

Sonuç

Mesleki Eğitim ve Öğretim kurumlarında Dijital Hijyen müfredatı için tasarlanan değerlendirme ve geri bildirim mekanizmaları, eğitim hedeflerine ulaşılmasını sağlamanın ayrılmaz bir parçasıdır. Program, çeşitli değerlendirme stratejileri ve çok kanallı geri bildirim sistemleri kullanarak sadece öğrenci öğrenimini etkili bir şekilde değerlendirmekle kalmaz, aynı zamanda öğretim yöntemlerini ve müfredat tasarımını da sürekli olarak geliştirir. Bu dinamik yaklaşım, müfredatın öğrencileri gerçek dünyadaki dijital hijyen zorluklarının üstesinden gelmeye hazırlamada ilgili ve etkili kalmasını sağlar.

Ünite 4- Mesleki Eğitim ve Öğretim Kurumlarından İyi Uygulamalar

Giriş

Dijital Hijyen gibi dinamik bir alanda, pratik uygulamalarla eşleştirilmiş teorik bilgiler en etkili öğrenme ortamını yaratır. Bu ünite, dijital hijyen ilkelerini müfredatlarına başarıyla entegre eden Mesleki Eğitim ve Öğretim (VET) kurumları tarafından benimsenen iyi uygulamaları incelemektedir. Bu vaka çalışmaları, dijital hijyen programlarının geliştirilmesi ve iyileştirilmesi için ölçüt görevi görmekte ve diğer kurumlar tarafından tekrarlanabilecek veya uyarlanabilecek başarılı stratejiler ve metodolojiler hakkında içgörü sağlamaktadır.

Örnek Çalışma 1: CyberVET Akademisi

Genel bakış:

CyberVET Academy, titiz akademisyenleri gerçek dünya uygulamalarıyla birleştiren sağlam dijital hijyen müfredatıyla tanınmaktadır. Bu kurum, gelişmekte olan teknolojilerin ve siber güvenlikle ilgili en iyi uygulamaların mesleki eğitime sorunsuz bir şekilde nasıl entegre edilebileceğine dair bir model haline gelmiştir.

Temel Stratejiler:

- Endüstri Ortaklıkları: CyberVET, müfredatlarının mevcut endüstri standartları ve uygulamalarıyla uyumlu olmasını sağlamak için önde gelen teknoloji şirketleriyle ortaklıklar kurmuştur. Bu ortaklıklar ayrıca misafir dersler, stajlar ve en son teknolojiye erişimi kolaylaştırmaktadır.
- Simüle Edilmiş Öğrenme Ortamları: Akademi, öğrencilerin gerçek zamanlı siber tehditleri güvenli bir şekilde keşfedebilecekleri ve azaltabilecekleri son teknoloji simüle edilmiş siber güvenlik laboratuvarları oluşturmak için yatırım yapmıştır. Bu uygulamalı deneyim çok değerlidir.

Sonuçlar:

- Mezunların %90'ının mezuniyetten sonraki altı ay içinde siber güvenlik alanında iş bulmasıyla öğrencilerin istihdam edilebilirliğinde belirgin bir artış.
- Uygulamalı öğrenme yaklaşımı ve doğrudan endüstri katılımına atfedilen gelişmiş öğrenci katılımı ve memnuniyeti.

Örnek Çalışma 2: TechBridge Mesleki Eğitim ve Öğretim

Genel bakış:

TechBridge VET, dijital hijyen alanında giderek artan endişe alanları olan mobil cihaz yönetimi ve güvenliğine odaklanmasıyla öne çıkıyor.

Temel Stratejiler:

- Modüler Müfredat Tasarımı: TechBridge'deki müfredat son derece modülerdir ve öğrencilerin öğrenme yollarını kariyer hedeflerine ve teknolojik gelişmelere göre uyarlamalarına olanak tanır.
- Toplum Projeleri: Öğrenciler, yerel küçük işletmelerin dijital güvenlik önlemlerini iyileştirmelerine yardımcı olmak için bilgilerini uyguladıkları sosyal yardım programlarına katılırlar.

Sonuçlar:

- Topluluk projeleri sadece öğrencilerin pratik becerilerini artırmakla kalmadı, aynı zamanda yerel küçük işletme sahipleri arasında siber güvenlik farkındalığını da artırdı.
- Modüler yaklaşım, eğitimde yüksek esneklik sağlayarak teknoloji ve öğrenci ihtiyaçlarındaki hızlı değişikliklere uyum sağlamıştır.

Örnek Çalışma 3: SecurePath Enstitüsü

Genel bakış:

SecurePath Institute, dijital hijyeni mesleki programlarına entegre ederek siber güvenliğin çeşitli teknik disiplinler için ne kadar temel olduğunu göstermiştir.

Temel Stratejiler:

- Disiplinlerarası Yaklaşım: SecurePath, dijital hijyen derslerini sağlık hizmetleri, otomotiv teknolojisi ve işletme yönetimi gibi programlara entegre ederek tüm öğrencilerin kendi alanlarında siber güvenliğin önemini kavramalarını sağlar.
- Sürekli Müfredat Değerlendirmesi: Enstitü, müfredatını en son siber tehdit istihbaratı ve sektör trendlerine göre sürekli olarak değerlendirmek ve güncellemek için yapay zeka odaklı bir analiz sistemi kullanmaktadır.

Sonuçlar:

- Teknoloji dışı programlardan gelen öğrenciler, dijital hijyen konusunda güçlü bir anlayışa sahip olarak mezun olurlar, bu da onları çok yönlü ve işverenler için daha çekici hale getirir.

- Sürekli müfredat değerlendirmesi, SecurePath'i dijital hijyen eğitiminin ön saflarında tutmuş ve ortaya çıkan tehditlere hızla uyum sağlamıştır.

En İyi Uygulamalar için Çıkarımlar

Bu kurumların başarıları, diğer MEÖ sağlayıcıları tarafından benimsenebilecek veya uyarlanabilecek bazı en iyi uygulamaları göstermektedir:

- Endüstri İşbirliği: Endüstri ile güçlü bağlar, müfredatı güncel tutmanın yanı sıra öğrencilerin mezuniyet sonrası iş bulma olanaklarını da artırmaktadır.
- Pratik Uygulama: Laboratuvarlar, simülasyonlar veya topluluk projeleri aracılığıyla uygulamalı öğrenme, dijital hijyen ilkelerini etkili bir şekilde anlamak ve uygulamak için çok önemlidir.
- Esneklik ve Disiplinlerarasılık: Esnek ve disiplinler arası bir yaklaşım, dijital hijyen eğitiminin değişikliklere hızla adapte olabilmesini ve çok çeşitli mesleki alanlara hitap edebilmesini sağlar.
- Geri Bildirim ve Sürekli İyileştirme: Öğrenciler, öğretim üyeleri ve sektör ortakları dahil olmak üzere çeşitli paydaşlardan gelen geri bildirimlere dayalı olarak müfredatın sürekli değerlendirilmesi ve revizyonu, programın etkinliğini ve uygunluğunu sağlar.

Örnek Çalışma 4: DigitalDefenders College

Genel bakış:

DigitalDefenders College, özellikle etik bilgisayar korsanlığı ve dijital adli tıp tekniklerini vurgulayarak siber güvenliği öğretmeye yönelik özel yaklaşımıyla tanınmaktadır. Bu mesleki eğitim kurumu, modern dijital ortamda siber tehditlerin karmaşıklığıyla mücadele etmeye hazır yetenekli profesyoneller yetiştirmeye kendini adamıştır.

Temel Stratejiler:

- Etik Bilgisayar Korsanlığı Modülleri: Etik bilgisayar korsanlığı üzerine kapsamlı modüller içeren kolej, öğrencilere kontrollü, etik ve yasal bir çerçevede sistem açıklarını belirleme ve kullanma becerileri kazandırır.
- Gerçek Dünya Siber Adli Tıp: Öğrenciler, gerçek dünyadaki veri ihlali senaryolarını taklit eden pratik siber adli tıp alıştırmalarına katılarak ihlallerin nasıl etkili bir şekilde izleneceğini, analiz edileceğini ve azaltılacağını anlamalarına yardımcı olur.

Sonuçlar:

- Mezunlar, siber güvenliğe proaktif yaklaşımlarıyla tanınmakta ve birçoğu finans ve devlet gibi yüksek riskli sektörlerde pozisyon elde etmektedir.
- Etik bilgisayar korsanlığı ve siber adli tıp alanındaki uygulamalı deneyim, öğrenciler arasında yüksek bir katılım düzeyine yol açmış ve siber tehditlerin pratik sonuçları hakkında derin bir anlayış geliştirmiştir.

Örnek Çalışma 5: InnovateTech Enstitüsü

Genel bakış:

InnovateTech Institute, Yapay Zeka (AI) ve Makine Öğrenimi (ML) gibi ileri teknoloji trendlerini dijital hijyen müfredatına entegre ederek farkını ortaya koymuştur. Bu yaklaşım, öğrencileri giderek artan yapay zeka odaklı siber güvenlik ortamına hazırlamaktadır.

Temel Stratejiler:

- Yapay Zeka Odaklı Güvenlik Çözümleri: Öğrencilere sofistike siber güvenlik önlemleri geliştirirken yapay zeka ve makine öğrenimini kullanmayı öğretmek ve böylece ileri teknolojileri kullanan siber suçluların önüne geçmek.
- Teknoloji Şirketleriyle Ortak Projeler: Öğrenciler, teknoloji şirketleriyle işbirliği içinde projeler üzerinde çalışarak, sektördeki zorluklar ve talepler hakkında gerçek zamanlı içgörüler sağlayan yapay zeka tabanlı güvenlik çözümleri oluştururlar.

Sonuçlar:

- Öğrenciler, ortak şirketler tarafından benimsenen ve mevcut siber güvenlik çözümleri üzerindeki doğrudan etkilerini gösteren çeşitli yapay zeka tabanlı güvenlik araçları geliştirdiler.
- Yapay zeka ve makine öğreniminin dijital hijyen eğitimine entegrasyonu, müfredatı daha sağlam hale getirmekle kalmamış, aynı zamanda öğrencilerin teknoloji odaklı sektörlerde istihdam edilebilirliğini de önemli ölçüde artırmıştır.

İyi Uygulamaların Özeti

DigitalDefenders College ve InnovateTech Institute'un bu ek vaka çalışmaları, mesleki eğitim ve öğretim kurumlarında başarılı bir dijital hijyen müfredatının kritik yönlerini daha da güçlendirmektedir:

- Uzmanlaşma ve İleri Eğitim: Etik bilgisayar korsanlığı ve yapay zeka gibi siber güvenliğin yüksek talep gören alanlarında uzmanlık eğitimi sunan programlar, müfredatın alaka düzeyini ve çekiciliğini önemli ölçüde artırabilir.

- Gerçek Dünya Uygulaması: İster siber adli bilişim isterse işbirliğine dayalı endüstri projeleri aracılığıyla olsun, öğrenilen becerilerin pratik, gerçek dünyada uygulanması, öğrencilerin yalnızca teorik kavramlara aşina olmalarını değil, aynı zamanda bunları gerçek durumlarda uygulama konusunda da yetkin olmalarını sağlar.
- Yenilikçi ve Geleceğe Hazır Müfredat: Müfredatın en son teknolojik gelişmelerle uyumlu tutulması, öğrencileri ortaya çıkan tehditlere ve fırsatlara hazırlar ve onları mezuniyet sonrası üstlendikleri herhangi bir siber güvenlik rolünde değerli varlıklar haline getirir.
- Bu örnekler, dijital hijyen eğitimini etkili bir şekilde geliştirmek için uygulanabilecek çeşitli stratejileri sergilemekte ve her biri giderek karmaşıklaşan siber ortamda dijital varlıkları korumak için donanımlı profesyoneller yetiştirme hedefine benzersiz bir şekilde katkıda bulunmaktadır.

Sonuç

CyberVET Academy, TechBridge VET, SecurePath Institute, DigitalDefenders College ve InnovateTech Institute tarafından incelenen beş vaka çalışması, dijital hijyenin Mesleki Eğitim ve Öğretim (VET) müfredatına entegre edilmesinde başarılı strateji ve yaklaşımların zengin bir dokusunu sunmaktadır. Her kurum, kendine özgü odak noktası ve metodolojisiyle, öğrencileri modern dijital dünyada siber güvenliğin karmaşıklıklarını aşmaya hazırlamada pratik, sektörle uyumlu ve yenilikçi eğitimin çok önemli rolünün altını çiziyor.

Önemli Çıkarımlar ve En İyi Uygulamalar

- Sektörel İşbirliği ve Uyum: Tüm vaka çalışmalarında ortak bir tema, endüstri liderleri ve şirketlerle güçlü bağlar kurmanın önemidir. Bu ortaklıklar sadece müfredatı en son teknolojiler ve uygulamalarla güncel tutmakla kalmıyor, aynı zamanda stajlar, gerçek dünya projeleri ve endüstri standartlarına maruz kalma yoluyla öğrencilerin istihdam edilebilirliğini de artırıyor.
- Uygulamalı ve Pratik Deneyim: Her kurum, öğrenilen kavramların pratikte uygulanması gerektiğini vurgular. İster siber laboratuvarlar, ister simüle edilmiş ortamlar, isterse de gerçek dünyadaki adli soruşturmalar yoluyla olsun, uygulamalı deneyim çok önemlidir. Sadece teorik bilgiyi pekiştirmekle kalmaz, aynı zamanda öğrencileri kariyerlerinde karşılaşacakları gerçek dünya zorluklarına da hazırlar.
- Uzmanlaşmış Modüller ve İleri Düzey Eğitim: DigitalDefenders College gibi kurumlar, etik bilgisayar korsanlığı ve siber adli tıp gibi alanlarda uzmanlık eğitimi sunmanın faydalarını vurgulamaktadır. Benzer şekilde, InnovateTech Institute'un yapay zeka odaklı güvenlik çözümlerine odaklanması, en yeni teknolojileri müfredata entegre etmenin, öğrencileri siber güvenlikte gelecekteki trendlere ve yeniliklere hazırlamanın avantajını göstermektedir.

- Disiplinlerarası ve Esnek Öğrenme Yaklaşımları: SecurePath Institute'un dijital hijyeni çeşitli mesleki programlara entegre etmesi, siber güvenlik eğitiminin uygulanabilirliğini ve uygunluğunu genişleten disiplinler arası bir yaklaşımın değerini örneklemektedir. Ayrıca TechBridge VET'in modüler müfredat tasarımı, hızlı teknolojik değişikliklere ve çeşitli öğrenci ilgi alanlarına uyum sağlayarak daha fazla esneklik sağlar.
- Sürekli İyileştirme ve Uyarlama: SecurePath Enstitüsü'nün sürekli müfredat değerlendirmesi için yapay zekaya dayalı analitiği kullanması ve InnovateTech Enstitüsü'nün dinamik güncelleme protokolleri, sürekli değerlendirme ve uyarlamanın önemini vurgulamaktadır. Müfredatın gelişen siber tehdit ortamına duyarlı tutulması, eğitim programlarının güncel ve etkili kalmasını sağlar.

Bu farklı mesleki eğitim ve öğretim kurumlarından elde edilen içgörülerin sentezi, bir dijital hijyen müfredatının etkinliğinin, teorik bilgiyi pratik becerilerle harmanlama, teknolojik gelişmelere uyum sağlama ve güçlü endüstri bağlantılarını teşvik etme becerisine bağlı olduğunu ortaya koymaktadır. Bu unsurlar, öğrencileri sadece siber güvenlik alanının mevcut taleplerini karşılamaya değil, aynı zamanda gelecekteki zorluklar karşısında yenilik yapmaya ve liderlik etmeye hazırlamak için çok önemlidir. Bu bütüncül yaklaşım sadece öğrenme deneyimini geliştirmekle kalmaz, aynı zamanda mezunların istihdam edilebilirliğini ve küresel olarak bağlantılı bir dünyada dijital varlıkları korumaya hazır olmalarını da önemli ölçüde artırır. Mesleki Eğitim ve Öğretim kurumları programlarını geliştirmeye ve iyileştirmeye devam ederken, bu vaka çalışmalarından çıkarılan dersler, yarının siber güvenlik ortamının zorluklarını karşılayacak donanıma sahip sağlam, kapsamlı dijital hijyen müfredatının geliştirilmesi için değerli planlar sunmaktadır.

Kaynaklar:

1. Stallings, W. (2017). *Kriptografi ve Ağ Güvenliği: İlkeler ve Uygulama* (7. baskı). Pearson Education.
2. Whitman, M. E., & Mattord, H. J. (2018). *Bilgi Güvenliği İlkeleri* (6. baskı). Cengage Learning.
3. Katz, J., & Lindell, Y. (2014). *Modern Kriptografiye Giriş* (2. baskı). CRC Press.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Kriptografi Mühendisliği: Tasarım İlkeleri ve Pratik Uygulamalar*. Wiley.
5. Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8. baskı). Sybex.
6. Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Yazılım Güvenliği Mühendisliği: Proje Yöneticileri için Bir Kılavuz*. Addison-Wesley Professional.
7. Conklin, W. A., White, G., Cothren, C., Williams, D., & Davis, R. (2016). *Bilgisayar Güvenliğinin İlkeleri: CompTIA Security+ ve Ötesi* (5. baskı). McGraw-Hill Education.
8. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Bilgisayarda Güvenlik* (5. baskı). Prentice Hall.
9. Bejtlich, R. (2013). *Ağ Güvenliği İzleme Uygulaması: Olay Tespiti ve Müdahaleyi Anlamak*. No Starch Press.
10. Zdziarski, J. A. (2015). *iOS Uygulamalarını Hacklemek ve Güvenliğini Sağlamak: Verilerin Çalınması, Yazılımların Ele Geçirilmesi ve Bunların Nasıl Önleneceği*. O'Reilly Media.
11. Tipton, H. F., & Nozaki, M. K. (2013). *CISSP CBK için Resmi (ISC)2 Kılavuzu* (4. baskı). CRC Press.
12. Peltier, T. R. (2016). *Bilgi Güvenliği Politikaları, Prosedürleri ve Standartları: Etkili Bilgi Güvenliği Yönetimi için Kılavuzlar*. Auerbach Yayınları.
13. Kim, D., & Solomon, M. G. (2016). *Bilgi Sistemleri Güvenliğinin Temelleri* (3. baskı). Jones & Bartlett Learning.
14. Caloyannides, M. A. (2010). *Gizliliğin Korunması ve Adli Bilişim* (2. baskı). Artech House.
15. Toigo, J. W. (2009). *Felaket Kurtarma Planlaması: Düşünülemez Olana Hazırlanmak* (3. baskı). Prentice Hall.
16. Ross, R. S. (2013). *Bilgi Güvenliği Risklerinin Yönetilmesi: OCTAVE (Operasyonel Kritik Tehdit, Varlık ve Zafiyet Değerlendirmesi) Yaklaşımı*. Addison-Wesley.
17. Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Tersine Aldatma: Organize Siber Tehditle Mücadele*. McGraw-Hill Osborne Media.
18. Enck, W. (2011). *Android Güvenliğini Anlamak*. IEEE Güvenlik ve Gizlilik Dergisi.
19. Anton, A. I., & Earp, J. B. (2004). *Bir Paydaş Tanımlama ve Belirginlik Teorisi: Kimin ve Neyin Gerçekten Önemli Olduğu İlkesinin Tanımlanması*. Academy of Management Review.
20. Liska, A., & Gallo, T. (2016). *Nesnelerin İnternetinin Güvenliğini Yeniden Düşünmek*. Elsevier.
21. Clarke, N. L., & Furnell, S. M. (2016). *Siber Güvenlik Eğitimi: Stratejiler ve En İyi Uygulamalar*. Springer.
22. Bishop, M. (2018). *Bilgisayar Güvenliği: Sanat ve Bilim*. Addison-Wesley.
23. Eckert, J. W. (2017). *CompTIA Linux+ Linux Sertifikasyon Kılavuzu*. Cengage Learning.

24. Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: Bilgisayar Saldırıları ve Etkili Savunmalar için Adım Adım Kılavuz*. Prentice Hall.

25. Easttom, C. (2019). *Modern Kriptografi: Şifreleme ve Bilgi Güvenliği için Uygulamalı Matematik*. McGraw-Hill Eğitim.

26. Kurose, J. F., & Ross, K. W. (2017). *Bilgisayar Ağları: A Top-Down Approach* (7. baskı). Pearson.

27. Andress, J., & Winterfeld, S. (2014). *Siber Savaş: Güvenlik Uygulayıcıları için Teknikler, Taktikler ve Araçlar*. Syngress.

28. Goodrich, M. T., & Tamassia, R. (2019). *Bilgisayar Güvenliğine Giriş*. Pearson.

29. Dafoulas, G. A., & Maia, C. (2015). *Küresel Güvenlik, Emniyet ve Sürdürülebilirlik: Yarının Siber Güvenlik Zorlukları*. Springer.

Çevrimiçi kaynaklar ve web siteleri:

- Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA)
    - Web sitesi: https://www.cisa.gov/
    - CISA, siber güvenlik eğitimi ve farkındalığı için çok önemli olan kılavuzlar, araçlar ve uyarılar sunarak siber güvenliğin en iyi uygulamaları ve tehditleri hakkında zengin kaynaklar sağlar.
- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Çerçevesi
    - Web sitesi: https://www.nist.gov/cyberframework
    - NIST'in çerçevesi, siber güvenlik risklerini yönetmek için yaygın olarak kullanılan bir standarttır ve eğitim müfredatlarına entegre edilebilecek yapılandırılmış bir rehberlik sağlar.
- Açık Web Uygulaması Güvenlik Projesi (OWASP)
    - Web sitesi: https://owasp.org/
    - OWASP, araçlar, standartlar ve en iyi uygulamalar da dahil olmak üzere web uygulama güvenliği konusunda ücretsiz ve açık kaynaklar sunan çevrimiçi bir topluluktur.
- SANS Enstitüsü
    - Web sitesi: https://www.sans.org/
    - Siber güvenlik eğitiminde tanınmış bir lider olan SANS Enstitüsü, çeşitli araştırma makaleleri, eğitim materyalleri ve güvenlik kılavuzları sunmaktadır.
- Krebs on Security
    - Web sitesi: https://krebsonsecurity.com/
    - Gazeteci Brian Krebs tarafından yönetilen bu blog, en son tehditlere ve ihlallere odaklanarak derinlemesine güvenlik haberleri ve araştırmaları sunuyor.
- Infosec Enstitüsü
    - Web sitesi: https://resources.infosecinstitute.com/

- Infosec Institute, kapsamlı makaleler ve sektör güncellemeleri de dahil olmak üzere bilgi güvenliğine odaklanan kaynaklar ve eğitimler sağlar.

- The Hacker News
  - Web sitesi: https://thehackernews.com/
  - Çevrimiçi bir siber güvenlik haber dergisi olan The Hacker News, güncel siber güvenlik tehditleri ve yenilikleri hakkında güncel bilgiler sunmaktadır.

- Bruce Schneier'in Blogu
  - Web sitesi: https://www.schneier.com/
  - Bruce Schneier, blogunda dijital dünyadaki güvenlik ve gizlilik konularına ilişkin görüşler sunan ünlü bir güvenlik teknolojisi uzmanıdır.

Modül 3: Uygulama ve Sürdürme

Ünite 1 - Girişimlerde ve Mesleki Eğitim Kurumlarında Dijital Hijyen Kültürü Oluşturma

Dijital Hijyen Kültürü Nedir?

Önceki modüllerde keşfettiğimiz gibi, Dijital Hijyen, ilk olarak bir sistemin verilerini, gizliliğini ve bütünlüğünü etkili bir şekilde korumayı amaçlayan güvenli, düzenli ve etik dijital uygulamalara yönelik ilkeleri açıklamak için ortaya çıkan bir terimdir [1]. Bu modülde, Avrupa'daki Mesleki Eğitim ve Öğretim sağlayıcıları için özelleştirilmiş bu ilkelerin daha büyük ölçekte sistemik uygulamasını keşfedecek ve kuruluşlarda inovasyon ve coşkuya ilham verecek daha iyi bir dijital hijyen kültürü oluşturmaya yönelik öneriler sunacağız.

Peki, dijital hijyen kültürü tam olarak nedir? İster yapı ister keşif merkezli olsun, başarılı bir organizasyon için çabalayan diğer birçok ağ kültürüne benzer şekilde [2] dijital hijyen kültürü ortak bir zihniyet etrafında şekillenir. Bu zihniyette, her üye kuruluşun misyonuna inanır ve kolektif sorumluluğa dayanan ve güvenli dijital uygulamaları entegre eden stratejiler formüle eder.

Dijital hijyen kültürünün liderlik seviyesinden çalışma gruplarına ve her bireye nasıl yayılabileceğini keşfedelim.

Liderlik Seviyesinde Dijital Hijyen Kültürünün Geliştirilmesi

Uzaktan çalışmanın yeni normal olduğu Covid sonrası dönemde, dijital dünyadaki güvenlik açıkları teknik olduğu kadar duygusal da olabiliyor [3] (örneğin, kimlik avı girişimi olan duygusal bir hikaye şeklini alabilen sosyal mühendislik saldırıları), durum yalnızca bir yöneticiyi değil, dijital dünyanın karmaşıklıklarını verimli bir şekilde yönlendirebilen ve aynı zamanda dijital hijyen uygulamalarını kurumsal değerlerin ayrılmaz bir parçası olarak gösteren bir lideri gerektirmektedir. Aşağıda bir liderin güvenli ve destekleyici bir dijital hijyen kültürünü teşvik edebileceği bazı önemli noktalar yer almaktadır:

- **Organizasyonel** Esnekliği **Teşvik Edin** [4]:

Liderler, kuruluşlarının dijital gelişmelerin yanı sıra dijital uygulamalar nedeniyle ortaya çıkabilecek zorluklara da uyum sağlayabilmesini sağlamalıdır. Ekiplerine bu değişimlerde rehberlik etmek için tüm liderler öncelikle konumlarını, kararlarını ve duygularını anlamalıdır [5] Ortak bir hedef doğrultusunda diğerlerini motive etmeden önce farklı koşullarda.

- **Yönetim Zorluklarının Ele Alınması** [5]**:**

Herhangi bir kuruluştaki liderler, siber güvenlik tehditleri, gizlilik endişeleri, beceri eksiklikleri veya uzaktan çalışmanın ortaya çıkardığı sorunlar gibi dijitalleşmeden kaynaklanabilecek potansiyel yönetim zorluklarının farkında olmalıdır. Ekiplerinin dijital hijyeni sağlama konusundaki yeteneklerini değerlendirmeye hazır olmalıdırlar. Bu, belirli bir düzeyde teknik uzmanlık gerektirir; bu nedenle liderlerin teknik konuları anlayabilmeleri ve ekiplerine etkili bir şekilde ifade edebilmeleri tavsiye edilir.

- **İlişkiler ve İşbirliğine Dayalı Süreçler Oluşturma 6:**

Herhangi bir kuruluştaki liderler hem iç hem de dış düzeyde çok çeşitli paydaşlarla ilişkiler kurmalıdır. Bu da yüksek düzeyde koordineli ve hesap verebilir olmalarının yanı sıra çalışanlar ve diğer paydaşlar arasında güçlü bir işbirliği duygusunu teşvik etmek için sorumluluk almalarını gerektirir.

- **Eğitim ve Öğretime Yatırım Yapmak [5]:**

Herhangi bir kuruluştaki liderler, en son dijital hijyen uygulamaları ve teknolojileri konusunda güncel kalmak için kendilerinin ve çalışanlarının sürekli eğitim ve öğretimine yatırım yapmalıdır. Bazı siber güvenlik şirketleri [7]Avrupa Birliği Siber Güvenlik Ajansı (ENISA) gibi Avrupa'daki bazı devlet kurumlarının yanı sıra, siber güvenlik farkındalığı ve kriz yönetimi konularında çeşitli çevrimiçi ve yüz yüze kurslar sunmaktadır [8].

Grup Düzeyinde Dijital Hijyen Kültürünün Geliştirilmesi

Dijital hijyen stratejisi için bir yol haritası belirlendikten sonra, herhangi bir kurumun siber güvenlik endişeleri grup düzeyinde de ele alınmalıdır. Departmanlar, programlar, öğrenciler veya proje yöneticileri dahil olmak üzere çalışma grupları, ilgili Bilgisayar Acil Durum Müdahale Ekiplerinin (CERT'ler) [Bu terimi Sözlüğe ekleyin] desteği ve işbirliği ile kurumlarında dijital hijyen kültürünün geliştirilmesine önemli ölçüde katkıda bulunabilir.

Aşağıda her bir çalışma grubunun dijital hijyen kültürü oluşturmak için yararlanabileceği bazı önemli noktalar yer almaktadır:

- **Gruplarda Etkili İletişim Kurma:**

Gruplar için etkili bir iletişim yöntemi, toplantılara veya kurslara siber güvenlikle ilgili tartışmalarla başlamaktır. Her grup başlangıçta üyelerin soruları için beş dakika ayırabilir. Bu toplantılar sırasında, dijital hijyen kültürünü güçlendirmek için cihazların departmanlarda veya sınıflarda nasıl kullanılması gerektiğine dair kurallar ve yönergeler daha da oluşturulabilir [9].

Gruplar için bir başka yararlı yöntem de, bir e-postanın veya dijital bir işlemin bir grup üyesi tarafından yapılıp yapılmadığını belirleyebilen paylaşılan belgeler için elektronik imzalar veya QR kodları gerektirmek olabilir [10]. Dikkat edilmesi gereken bir diğer faktör de USB flash sürücüler yerine bulut gibi daha güvenli depolama seçeneklerinin tercih edilmesidir [10].

- **Dijital Saldırılar için Etkin Belgeleme Yöntemlerinin Oluşturulması:**

Dijital saldırıların belgelenmesi siber güvenliğin sağlanmasında kritik bir unsurdur. Tüm kuruluşlar dokümantasyona ilişkin yönergeleri açıkça açıklamalıdır. Dijital saldırılar için dokümantasyon geliştirmeye yönelik bazı prosedürler aşağıdaki gibi olabilir [11]:

ADIM 1: Düzenli Bir Günlük Tutun: Bir olay durumunda, ekibinizin her üyesini tarih, saat, e-posta adresi, ilgili bağlantılar, hesap adları ve meta veriler gibi veri noktalarını dahil etmeye teşvik edin.

ADIM 2: Yapılandırılmış Şablonları Uygulayın: Veri ihlali olaylarını belgelemek için hazır şablonlar kullanın. Örneğin, dünya çapında insanların dijital medeni haklarını korumayı amaçlayan uluslararası bir STK olan Access Now'ın olay günlüğü şablonunu kullanabilirsiniz.

ADIM 3: Farklı Belgeleme Formatları Kullanın: Ekip üyelerinizi sorunlarını belgelemek için çeşitli formatlar kullanmaya teşvik edin. Bir web sayfasını kaydetmek için İnternet Arşivi'nin Wayback Makinesi'ni kullanabilir veya sorunlarının kanıtı olarak video kaydetmek için video yakalama araçlarını kullanabilirler.

ADIM 4: Bilgileri Güvenli Bir Şekilde Saklayın: Kendi cihazlarınızda, güvenilir depolama seçeneklerinde yedekler oluşturun ve mümkünse dosyalarınızı şifreleme ile koruyun.

- **Düzenli Dijital Hijyen Değerlendirmelerinin Oluşturulması:**

Düzenli denetimler ve risk değerlendirmeleri yapmak, güvenlik açıklarının belirlenmesine ve dijital hijyen uygulamalarına uyulmasının sağlanmasına yardımcı olabilir [11]. Düzenli dijital hijyen değerlendirmeleri oluşturmanın bazı yolları aşağıdaki gibidir:

- Virüs taraması yapmak, şifreleri değiştirmek, yazılımları güncellemek ve sabit diskleri temizlemek gibi siber hijyen alışkanlıklarından oluşan bir rutin geliştirmek [12].
- Ağ güvenlik duvarı, antivirüs yazılımı, şifreleme veya yedekleme çözümleri gibi doğru araçların kullanılması [13].
- Güvenlik açığı taraması, web uygulaması taraması ve kimlik avı değerlendirmeleri sağlayan güvenilir hizmetlerden yardım alın [14].

Bireysel Düzeyde Dijital Hijyen Kültürünün Geliştirilmesi

İnsan faktörleri siber güvenliğin en zayıf bileşenlerinden biridir. Dijital uygulamalar açısından bazı insan hatası örnekleri arasında Kötü şifre yönetimi, yanlışlıkla veri silme veya kimlik avı veya diğer sosyal mühendislik dolandırıcılıklarının kurbanı olma sayılabilir. Ancak, dikkat ederek ve dijital hijyen uygulamalarını takip ederek riskleri azaltmak her zaman mümkündür.

İşte her bireyin bir kurum içinde hijyen kültürü yaratılmasına katkıda bulunabileceği bazı kilit noktalar:

- **Dijital Ayak İziniz Konusunda Dikkatli Olun [15]:**

Çevrimiçi alanlarda gezinmek karmaşık olabilir ve insanlar dijital ayak izleri konusunda dikkatli olmalıdır. Web tarayıcılarının, e-posta sağlayıcılarının, mobil uygulamaların, arama motorlarının ve sosyal medya platformlarının izleme mekanizmaları kişisel gizliliği tehlikeye atabilir. Günlük web tarama faaliyetlerinde güvenliği artırmak için aşağıdaki adımları göz önünde bulundurun:

ADIM 1: Sosyal platformlarda paylaşılan bilgilere dikkat edin ve sosyal medya hesaplarınızdan çıkış yapın, çünkü sosyal medya siteleri siz kullanmasanız bile hesaplarınız üzerinde analizler yapabilir [16].

ADIM 2: duckduckgo.com ve startpage.com gibi gizliliğe öncelik veren ve kullanıcılara kişiselleştirilmiş izleme olmadan arama sonuçları sağlayan tarayıcıları kullanın.

ADIM 3: Sosyal çevrenizin çevrimiçi faaliyetlerinin farkında olun[16]: Arkadaşlarınızın ve ailenizin çevrimiçi varlığının dijital güvenliğinizi etkileyebileceğinin farkında olun. Onlara güvenli çevrimiçi uygulamalar konusunda tavsiyelerde bulunun.

ADIM 4: Akıllı telefon ayarlarınızın farkında olun: Tıpkı dizüstü bilgisayarlarınız gibi akıllı telefonlarınız da çevrimiçi faaliyetlerinizin önemli bir parçasıdır. Hassas bilgiler taşıyan uygulamalardan sürekli olarak çıkış yaparak güvenliğe öncelik verin. Oturumu kapatmak iş verimliliğiniz için de faydalı olacaktır. Akıllı telefon kullanımının izlenmesi üzerine yapılan bir çalışma oturumu kapatarak ve izleme çerezlerini devre dışı bırakarak katılımcıların her oturumda daha az zaman harcadığını ortaya koymuştur [17].

- **Yazılım Güncellemelerine Dikkat Edin:**

Yazılımınızı veya web tarayıcılarınızı güncellememek ciddi güvenlik açıklarına neden olabileceğinden, sık yazılım güncellemeleri iyi bir dijital hijyen için gereklidir.

Yazılım güncellemelerinin önemini gösteren yakın tarihli bir örnek, Adobe'nin Flash'ı durdurduğunu açıkladığı 2021 yılında ortaya çıktı ve bu kararda güvenlik açıkları büyük rol oynadı [18]. Söz konusu güvenlik açıkları, web tarayıcısı güvenlik önlemlerinin etkin bir şekilde atlanabilmesini içeriyordu. Bilgisayar acil müdahale ekipleri (CERTs) sorunları ele almak zorunda kaldı. Bu örnekte de görüldüğü gibi, güncellemelere dikkat etmek yazılım ve uygulamalarınızı güvenlik açıklarından korumanın önemli bir parçasıdır.

- **Güçlü Parolalar Kullanın[19]:**

Kolayca tahmin edilebilen zayıf parolalar, bireyleri ve kuruluşları veri ihlali riskiyle karşı karşıya bırakabilir. Bu nedenle, adınızı veya doğum gününüzü parola olarak kullanmayın. En güçlü parolalar hatırlanması kolay ancak kırılması zor olanlardır. İşte güçlü parolalar oluşturma ve bunları hatırlama konusunda bazı ipuçları[19]:

ADIM 1: Büyük ve küçük harfleri içerecek şekilde farklı sembollerle bir cümle oluşturun. Örneğin, "Elmaları severim ama portakallardan nefret ederim" gibi bir cümle "IL@bIH0" şekline dönüştürülebilir.

ADIM 2: İki faktörlü kimlik doğrulama kullanın: Sağlam parolalar oluşturmanın yanı sıra, iki faktörlü kimlik doğrulama (2FA) ile güvenliğinizi artırın. Kimlik doğrulama, mobil cihazınıza gönderilen bir kod gibi ikinci bir doğrulama adımı gerektirerek ekstra bir güvenlik katmanı ekler ve bu da yetkili erişim riskini azaltır.

ADIM 3: Şifrelerinizi gizli tutun ve gerekirse bir şifre yöneticisi veya Dashlane veya 1Password gibi bir kimlik doğrulayıcı uygulama ile güvenli bir şekilde saklayın. (Ancak, bu yöneticilerin güvenliğinin yalnızca en zayıf halkaları kadar güçlü olduğunu unutmayın!)

ADIM 4: Parolalarınızı düzenli olarak güncelleyerek güvenliğini sağlayın.

- **Dikkatli Tıklamalar: Kimlik Avına Karşı Dikkatli Olun[14]:**

Oltalama, güvenilir bir kaynak gibi davranarak insanları hassas bilgilerini vermeleri için kandırmayı amaçlar. Oltalama ciddi bir suçtur. Dolandırıcılar insanları kişisel bilgilerini vermeleri için kandırırlarsa, e-posta, banka veya sosyal medya hesaplarına erişebilirler. Bu nedenle, bir şey biraz sıra dışı görünüyorsa veya bir e-posta sizden kişisel bilgilerinizi doğrulamanızı istiyorsa, özellikle de bir ek veya tıklamanızı istedikleri bir bağlantı varsa, öncelikle içgüdülerinize güvenin ve tıklamadan önce düşünün.

Ünite 2 - Dijital Hijyen Uygulamalarının İzlenmesi, Gözden Geçirilmesi ve Sürekli İyileştirilmesi

Dijital varlığınızı eviniz ya da arabanız gibi değerli bir varlık olarak düşünün. Arabanızı ya da evinizi güvenli ve işlevsel tutmak için nasıl düzenli bakım seansları yapmanız gerekiyorsa, aynı şekilde dijital hijyen uygulamalarınızı kontrol etmek de sistemlerinizi sürekli olarak güvenli ve işlevsel tutmak için önemlidir. Bu ünitede, teknoloji geliştikçe yetkinliklerinizi güncel tutmak için kurumsal ve bireysel düzeyde gerçekleştirebileceğiniz uygulamaları inceleyeceğiz.

Kurumsal Düzeyde Uygulamalar

İşte kurumsal düzeyde dijital hijyeninizi izlemek, değerlendirmek ve iyileştirmek için yardımcı olabilecek araç ve yöntemlerden bazıları.

- **En son AB Yönetmeliklerini bulun:**

En son düzenlemelerin anlaşılması ve uygulanması, kurumların en acil sorunları belirlemelerine ve tehditleri azaltmak ve faydalardan yararlanmak için buna göre hareket etmelerine yardımcı olur.

Politika yapıcıların endişe duyduğu en ciddi zorluklardan biri yapay zekadır. Avrupa Birliği, 9 Aralık 2023 tarihinde, "teknolojinin potansiyel faydalarından yararlanırken, işlerin otomatikleştirilmesi gibi olası risklerinden korunmayı" amaçlayan "AI Act" adlı yeni bir yasa çıkardı.[20]." Yapay zeka ile ilgili en son Avrupa Birliği düzenlemelerinden haberdar olmak, sorumlu ve yetkili dijital uygulamalar için çok önemlidir. Yönergelere uyum sağlamak ve olası yasal sonuçlardan kaçınmak için Yapay Zeka Yasası gibi güncellenmiş düzenlemeleri Avrupa Birliği'nin mevzuatlar sayfasından çevrimiçi olarak inceleyebilirsiniz.

- **Güvenlik Kontrolleri:**

Güvenlik ayarlarınızı kapsamlı bir şekilde gözden geçirmek, dijital hijyen yönergelerinizin verimliliğini izlemek açısından çok önemlidir. Google ve Facebook'un gizlilik önlemleri, izinler ve en son faaliyetlerinizin kontrolü konusunda size rehberlik eden rutin güvenlik kontrollerini kullanabilirsiniz. Ayrıca, veri ihlallerinin risklerinden ve sıklığından haberdar olmak için haveibeenpwnd.com gibi birden fazla veri ihlalini araştırmanıza olanak tanıyan çevrimiçi kaynakları da kullanabilirsiniz.

- **SWOT Analizi:**

SWOT, Güçlü Yönler, Zayıf Yönler, Fırsatlar ve Tehditlerin kısaltmasıdır ve herhangi bir kuruluşun konumunu ve gelecekteki gelişim stratejilerini tanımlamak için bir yol haritası oluşturacak stratejik bir analiz yöntemidir.

İşletmelerin e-hazırlığı üzerine yapılan bir araştırmaya göre, kuruluşunuz için bir SWOT Analizi yaparken aklınızda bulundurmanız gereken bazı ipuçları şunlardır[21]:

1. **SWOT Analizi için Hazırlık:**
    a. BİR AMAÇLA BAŞLAYIN: SWOT analizi uygulamanın amacını ve uzun vadeli etkilerini göz önünde bulundurun.
    b. ANALİZ EDİLECEK ALANLARI TANIMLAYIN: Dijital Hijyen Kültürü ile ilgili belirli alanları belirleyin, örneğin çalışan farkındalığı, güvenlik protokollerinin takibi, altyapı vb.
    c. EKİPLERİ TANIMLANAN ALANLARA GÖREVLENDİRİN: Analiz etmek istediğiniz alanlarda uzman ekipler oluşturun ve tüm farklı ekiplerin analizin yürütülmesine ilişkin metodoloji konusunda uyumlu olmasını sağlayın
2. **Güçlü ve Zayıf Yönler Analizi:**
    a. GÜÇLÜ ve ZAYIF YÖNLERİNİZİ BELİRLEYİN: Bir kuruluşun güçlü ve zayıf yönleri, o kuruluşun etkinliğini ve etkinsizliğini gösteren iç faktörlerin işaretleridir. Zayıflık olarak değerlendirilecek belirli bir faktöre ilişkin kararların gerekçelerini de dahil etmek önemlidir. (Örneğin, güncelliğini yitirmiş uygulamalar, sistemlerin saldırıya açık olması nedeniyle bir zayıflık olarak değerlendirilebilir).
    b. BELIRLENEN KONULARIN UYGUNLUĞUNU BELIRLEMEK: Neyin zayıflık, neyin güçlü yön olduğunu belirlemek kafa karıştırıcı olabilir. Araştırmacılar şunları önermektedir [21] değerlendirmek ve önceliklendirmek için '100 puan Yöntemi'ni kullanır. Her ekip üyesi bir güçlü veya zayıf yöne 100 puan verebilir ve ne kadar çok puan verilirse o kadar önemli kabul edilir. Herkes puanlarını verdikten sonra, ekip genel önemlerini belirlemek için bunların ortalamasını alır.
3. **Fırsatlar ve Tehditler Analizi:**
    a. Tehditlerin uygunluğunu ve olasılığını şu kategorilerde düzenlemeye çalışarak değerlendirin: ekonomik, sosyal, siyasi, teknolojik ve çevresel.
    b. Her bir gelişmeyle ilişkili fırsatları hesaplayın. Bunlar mali kaynaklar, kamu ilgisinde artış veya uluslararası fırsatlar olabilir.
4. **SWOT Matrisinin Geliştirilmesi:** Güçlü yönleri, zayıf yönleri, fırsatları ve tehditleri seçin ve bunları kuruluşunuzun Dijital Hijyen Kültürü için en yüksek öneme göre gruplandırın. Belirlenen stratejilere dayalı eylem planları geliştirin: (1) fırsatlarınızdan yararlanarak zayıflıkları düzeltmeye odaklanın, (2) bir fırsattan yararlanmak için bir güçten yararlanmaya odaklanın (3) bir tehditten kaçınmak için bir zayıflığı en aza indirmeye odaklanın veya (4) bir tehdidi önlemek için bir güçten yararlanmaya odaklanın.
5. **Sonuçlarınızı gözden geçirin**: Uygulanan stratejilerin ilerleyişini düzenli olarak gözden geçirin ve dijital ortamdaki yeni gelişmelere uyum sağlamak için SWOT analizini periyodik olarak yineleyin.
    - **Düzenli BackUp'lar:**

Parola kaybı, teknik olaylar vb. durumlarda hassas bilgilerin kurtarılmasına ihtiyaç duyulduğunda yedeklemeler çok önemlidir. Bazen, sistemdeki güvenlik açıklarını veya hataları gözden geçirerek bir sistem çökmesinin nedenlerini izlemek de mümkündür. Belgelerinizin bir kopyasını saklamanızı sağlayan UrBackUp gibi açık kaynaklı bir yedekleme sistemi kullanmak, acil bir durumda dijital hijyen uygulamalarınızı izlemek ve gözden geçirmek için değerli bir araç olabilir.

Bireysel Düzeyde Uygulamalar

Her birey dijital hijyen uygulamasının geliştirilmesinde önemli bir rol oynar ve mevcut uygulamalarınızı gözden geçirmek, izlemek ve geliştirmek için çok sayıda adım atılabilir. İşte dijital hijyeninizi bireysel düzeyde geliştirmenin bazı yolları.

- **Farkındalık ve Eğitim:**

Dijital okuryazarlığı benimsemek sadece araç ve yöntemleri bilmekle değil, aynı zamanda sürekli gelişen teknolojik ortamı anlamakla da ilgilidir. Kendimizi çevrimiçi tehditler konusunda eğitmek ve güncel kalmak, katılımcıların bilgisayarla çalışmak gibi dijital okuryazarlığın temellerinin yanı sıra çevrimiçi içerik oluşturmak gibi ileri düzey yetkinlikleri de öğrenebilecekleri Microsoft Dijital Okuryazarlık Kursları gibi sürekli öğrenme fırsatlarına katılım yoluyla sağlanabilir. Benzer şekilde, araştırmacılar[22] medya okuryazarlığı ve bireylerin gerçek yaşam deneyimlerini ve ilgi alanlarını yansıtması gereken güvenli ve sorumlu internet kullanımı hakkında öğretimin önemine işaret etmektedir.

- **Sorumlu Çevrimiçi Davranış:**

Çevrimiçi davranışlarımızın gerçek dünyada sonuçları vardır. Akademik çalışmalarda vurgulandığı gibi[23] dijital okuryazar olmanın yanı sıra çevrimiçi ortamda etik bir şekilde yer almak da kritik önem taşımaktadır. Sorumlu çevrimiçi davranış, çevrimiçi tartışmalara saygı ve duyarlılıkla katılmayı içerir. Ayrıca, dijital politikaların farkında olmak daha güvenli ve daha saygılı bir çevrimiçi topluluğa katkıda bulunur. Dijital eylemlerinizin iyi uygulamalar içerip içermediğinden emin değilseniz. Michigan Üniversitesi'nin İyi Dijital Vatandaş kılavuzunu kullanabilirsiniz.

- **İnceleme ve Uyarlama:**

Dijital dünyanın her alanında olduğu gibi, teknolojik ortam da dinamiktir ve uygulamalarımızı sürekli olarak uyarlamamızı gerektirir. Bu nedenle, dijital eylemlerimizi gözden geçirerek dolandırıcılıklara uyum sağlamak, kimlik avı girişimlerini fark etmek ve indirdiklerinize karşı dikkatli olmak, çevrimiçi güvenliği korumanın temel unsurlarıdır.

Uygulamaları gözden geçirmenize ve düzenli olarak güncellenmenize yardımcı olabilecek bir araç Dijital Yeterlilik Çerçevesi veya DigComp'tur. Kurumlar, bireyler ve eğitimciler için AB tarafından geliştirilen ve bu

el kitabının yayın tarihi itibariyle son versiyonu 2.2 ile güncellenmeye devam eden bir referans aracıdır. DigComp'a AB Yayınlarının web sitesinden ulaşılabilir.

DigComp'ta yapılan düzenli güncellemeler, çerçevenin güncel kalmasını ve mevcut dijital ortamı yansıtmasını sağlar. Tıpkı DigComp'ta olduğu gibi siz de dijital hijyen uygulamalarınızı gözden geçirip güncelleyerek kuruluşunuzun mevcut ihtiyaçlarıyla uyumlu olmalarını sağlayabilir ve gelişmekte olan teknolojilerle ilgili becerileri de dahil etmeyi düşünebilirsiniz.

Ünite 3 - Dijital Hijyenin Geleceği: Zorluklar ve Fırsatlar

Geleceğe doğru ilerlerken, teknolojik gelişmelerde yeni zorluklar ve fırsatlar görmemiz bekleniyor. Dijital teknolojilerin, özellikle de Yapay Zekanın (AI) gelişen manzarası, daha fazla yetenek ve beceri kazandıkça yeni karmaşıklıklar yaratıyor. Bu karmaşıklıkları ve fırsatları anlamak, herkes için güvenli, emniyetli ve yenilikçi bir deneyim sağlamak için çok önemlidir. Bu ünitede, dijital hijyenin geleceği için en acil konulardan bazılarına, özellikle de gelişmekte olan teknolojilere ve bunların inovasyon için neler getirebileceğine odaklanarak bakacağız.

A-Yükselen Teknolojiler

Blockchain, Robotik, Nesnelerin İnterneti (IoT), Artırılmış Gerçeklik (AR) ve Sanal Gerçeklik (VR) gibi gelişmekte olan birçok teknolojinin geleceği şekillendirmesi bekleniyor. Bunlar arasında, ChatGPT gibi Üretken Yapay Zeka sohbet robotları, 2022'deki başlangıcından bu yana en çok manşet olanlardır.

Yapay zekanın yükselişi dijital hijyen ve siber güvenliğe yeni boyutlar getiriyor. YZ teknolojileri "şimdiden soruları yanıtlayabiliyor, şiir yazabiliyor, bilgisayar kodu üretebiliyor ve konuşmalar yapabiliyor."[24] Bazı uzmanlar, işler otomatikleştirileceği için yapay zekanın birçok çalışanı riske atacağına inanıyor[25]Oysa birçok şirket uygulamaları için halihazırda üretken yapay zekayı kullanıyor[26]. Peki, Mesleki Eğitim ve Öğretim kurumları gibi bir eğitim kurumu yapay zekanın olanaklarından nasıl faydalanabilir?

- **Öğrenme Deneyiminin Geliştirilmesi:**

Mesleki Eğitim ve Öğretim alanında, üretici yapay zeka öğrenme deneyiminde devrim yaratma konusunda büyük bir potansiyele sahip olabilir. Araştırmacılar, YZ'nin öğrencinin ihtiyaçlarına, ilgi alanlarına ve yeteneklerine uygun gerçekçi senaryolar, simülasyonlar veya değerlendirmeler oluşturabileceğini öne sürüyor[27]. Gerçekçi senaryolar, sağlık hizmetleri gibi alanlar için çok önemli deneyimler yaratabilecek uygulamalı, sürükleyici deneyimler sunabilir. Buna ek olarak, sağlık hizmetleri eğitimi rutin görevleri optimize etmekten, teşhis koymaktan veya kişiselleştirilmiş tıp sunmaktan büyük fayda sağlayabilir; bu da gizlilik ve sağlam yönetişim etrafında konuşmalar yapılmasını gerektirir [28].

- **Öğretim ve Değerlendirmenin İyileştirilmesi:**

Endüstri Trendlerine uyum sağlamak ve yapay zekayı Mesleki Eğitim ve Öğretimde öğretim ve değerlendirmeye entegre etmek, eğitmenlerin iş akışlarını optimize etmelerine yardımcı olabilir. STK'lar ve uluslararası kuruluşlar, öğrencinin çalışmasının doğruluğunu, eksiksizliğini ve genel kalitesini iyileştirme olanaklarını şimdiden araştırıyor ve bu da anında geri bildirim sağlayabilir[29]. Tıpkı sağlık eğitiminde olduğu gibi, YZ'ye öğrenci çalışmalarını değerlendirme becerisi kazandırmak, şüphesiz YZ'nin etiğine ilişkin soruları gündeme getirecektir; bu da öğretmenlerin ve ebeveynlerin akıllarında tutmaları gereken önemli bir tartışma noktasıdır.

- **Uyarlanabilir Öğrenci Yönetim Sistemleri:**

Öğrenme Yönetim Sistemleri (LMS), öğretme ve öğrenme materyallerini tek bir yerde sunmanın yanı sıra öğrencinin ilerlemesini ve performansını takip ettiği için Mesleki Eğitim ve Öğretim öğretmenlerinin ufkunu şimdiden genişletmiştir[30]. Yapay zeka ile LMS, LMS'de devrim yaratma olasılığını artırdı [31]. Yapay zeka destekli LMS, öğrenci performansını tahmin etmeyi de içerebilen otomasyonun ötesinde gelişmiş görevler yapabilir, böylece öğretmenlerin öğrenci performansını iyileştirmek için stratejiler oluşturmasına olanak tanır [32]

B-Düzenleyici Zorluklar

Yukarıdaki ünitelerde, yeni teknolojik gelişmelerin çeşitli sektörlerde ve eğitim sistemlerinde nasıl oyunun kurallarını değiştirdiğini incelemiştik. Bu gelişmeler, tüm paydaşların yeni teknolojilerin daha güvenli kullanımı için sorumlu ve teşvik edici olmalarını gerektirmektedir. Veri gizliliği, algoritmik önyargı, etik kullanım ve hesap verebilirlik gibi konular kapsamlı düzenleyici çerçeveler gerektirmektedir.

- **Eğitimde Veri Gizliliği**

Eğitim bağlamında, özellikle de büyük miktarda veri işleyen çevrimiçi eğitim bağlamında, gizlilik ve güvenlikle ilgili endişeler vardır [33]. Bir buluta yetkisiz erişim veya hassas bilgilerin kötüye kullanımı eğitim kurumları için önemli bir risk oluşturmaktadır ve 2018'den bu yana, AB Genel Veri Koruma Yönetmeliği (GDPR), AB içindeki ve dışındaki tüm kuruluşların kişisel verilerin korunması ve taşınmasına yönelik itirazlarına uymasını zorunlu kılmıştır [34]. Bu nedenle, her Mesleki Eğitim ve Öğretim kurumunun GDPR ile uyumluluğunu izlemesi ve geliştikçe gerekli önlemleri alması teşvik edilmektedir.

- **Algoritmik Önyargı**

Yapay zeka destekli bir LMS, kendisini eğitmek için kullanılan verilerden önyargılar devralabilir. İstihdam açısından, tahmin sisteminin erkek adayların özgeçmişlerinin çoğunluğu ile eğitildiği bir Amazon işe alım sürecinde keşfedildiği gibi, AI destekli istihdam prosedürleri bazı gruplar için özellikle zararlı olabilir. Bu durum, erkek adayların kadın adaylara göre daha fazla tercih edildiği bir önyargı yaratmıştır [35]. Öğretmenler, yapay zeka destekli sistemlerin bu yönünün farkında olmalı ve öğrenciler hakkındaki kendi önyargılarını çapraz kontrol etmelidir. Politika yapıcıların denetlenebilir ve şeffaf algoritmaların geliştirilmesini teşvik etmeleri de giderek önem kazanmaktadır [36].

- **Gelişen Teknolojilerin Etiği**

Algoritmik önyargıya ilişkin endişelere benzer şekilde, yapay zeka gibi gelişmekte olan teknolojilerin eğitime entegrasyonu da önemli sorular ortaya çıkarmaktadır. Gelişmekte olan teknolojilerin karar verme açısından eğitimdeki rolü ne olmalıdır? Farklı öğrenci grupları arasında, gelişen teknolojilerin öğrenmelerini nasıl etkilediği konusunda önemli farklılıklar var mı?

Yapay zeka alanında araştırmacılar, gizlilik, önyargı, gözetim ve özerkliği, bu sistemlerin eğitimde kullanılmasına yönelik etik zorluklara işaret eden kilit alanlar olarak değerlendirmektedir [37]. Bu alanlar ve yukarıdaki örnek sorular, öğretmenlerin gelecek nesilleri yapay zekanın etik kullanımı ve geliştirilmesi konusunda eğitmeleri için daha fazla mesleki gelişim fırsatı gerektirmektedir. Bu bağlamda, AB'nin Dijital Yetkinlik Çerçevesi (DigComp) gibi girişimler değerli bir rehber olarak hizmet edebilir.

Etik YZ kullanımını teşvik etmenin öneminin farkında olan Avrupa Konseyi gibi yürütme organı, halihazırda etik yönergeleri tanımlama ve teknoloji şirketlerini sorumlu tutacak şeffaflığı teşvik etme sürecindedir. Avrupa Birliği, yukarıda bahsedilen YZ Yasası düzenlemesinin yanı sıra, vatandaşların yaşamları üzerinde daha büyük etkileri olması beklenen sanal gerçeklik, robotik ve biyoteknoloji gibi gelişmekte olan teknolojilerin kullanımını desteklemek ve teşvik etmek için politikalar da geliştirmektedir [38].

C-İnovasyon için Fırsatlar

2021 OECD Raporuna göre, Sanal Gerçeklik, Artırılmış Gerçeklik, Robotik ve Yapay Zeka, lojistik, tarım, konaklama, enerji ve bilgi teknolojileri gibi birçok sektör için Mesleki Eğitim ve Öğretimde giderek yaygınlaştı ve önümüzdeki yıllarda daha da yaygınlaşacak [39]. Bu bölümde, çeşitli sektörlerin bu teknolojilerden halihazırda nasıl yararlandığına ve ileride ne gibi potansiyeller olduğuna bakacağız.

- **Bilgi Teknolojileri (IT)**

Sanal gerçeklik bulut laboratuvarları gibi Gelişen Teknolojiler, BT öğrencilerine ağ yapılandırması veya siber güvenlik gibi çeşitli alanlarda uygulamalı deneyim sağlayabilir [40]. Siber Güvenlik Laboratuvarları [Sözlük Terimini Buraya Girin], siber tehditleri ve saldırıları simüle ederek Mesleki Eğitim ve Öğretim öğrencilerine gerçek dünya riskleri olmadan dijital sistemlerdeki güvenlik açıklarını anlamaları için pratik bir ortam sunar. Yüksek Performanslı Hesaplama [Sözlük Terimini Buraya Girin] ve Blockchain [Sözlük Terimini Buraya Girin] gibi sistemler, siber güvenlik için yeni eğitim yolları sunmaktadır [41].

- **Lojistik ve Taşımacılık**

Simülasyon oyunları gibi ticari ürünler, öğrencilerin gerçek dünyadaki zorlukların üstesinden gelmelerine yardımcı olabilir ve lojistik söz konusu olduğunda, piyasada bulunan Truck & Logistics Simulator adlı oyun tam olarak bunu yapıyor ve öğrenciler lojistik görevlerini başından sonuna kadar yerine getirebiliyor [39]. Teknoloji karmaşık görevlerin planlanmasında çok önemli bir rol oynadığından, mesleki eğitim ve öğretim sağlayıcıları, öğretmenler ve öğrencilerin iyi bir dijital hijyen uygulaması ve ticarileştirilmiş ürünlerle bilgi paylaşırken lojistik ağlardaki bilgilerin bütünlüğünü güvence altına alması gerekmektedir.

- **Tarım**

Drone'lardan yapay zekaya, yeni teknolojiler tarım ve çiftçilik uygulamalarının verimliliğini artırma, çevresel etkileri azaltma ve gelir artışı sağlama potansiyeline sahiptir. Daha yüksek çözünürlüklü drone araştırma

modelleri, daha verimli sulama planlaması ve daha hassas mahsul ve hayvan izleme ile sonuçlanabilir [42]. Benzer şekilde, AR akıllı tarımı ilerletmek için kullanılabilir [43] Tarım sektöründe riskleri en aza indirmeyi, mahsul verimini artırmayı ve stresi azaltmayı amaçlayan [44]. Bununla birlikte, bu teknolojilerden bazılarının kullanımıyla ilgili riskler de göz ardı edilmemelidir [45]. İyi bir siber hijyen sağlayarak ve sorumlu yapay zeka uygulamalarını dahil ederek yapay zeka, AR ve diğer gelişmekte olan teknolojileri kullanmanın riskleri azaltılabilir.

- **Misafirperverlik**

Otelcilik, Avrupa'daki birçok ülkede ekonomiye katkıda bulunan ve milyonlarca kişiye istihdam sağlayan önemli sektörlerden biridir. Gelişen teknolojiler, konaklama ve turizm öğrencileri için sürükleyici öğrenme deneyimleri sunabilir. Oda sıcaklığı, aydınlatma ve diğer özelliklerin kontrol edilmesini sağlayan Nesnelerin İnterneti [Sözlük Tanımını Buraya Ekleyin] tarafından desteklenen otel yönetimi simülasyonları ve müşteri hizmetleri senaryoları, misafirler için daha iyi deneyimler yaratabilir[46]. Kulaklık takılarak deneyimlenen VR eğitim modelleri, sektörün önde gelen konaklama liderleri tarafından halihazırda kullanılmaktadır [47]. Simüle edilmiş dünya deneyimi, insanların daha hızlı öğrenmelerine, bilgiyi daha uzun süre akıllarında tutmalarına ve eğitime daha fazla katılmalarına yardımcı olabilir [48]. Bu gelişmeler her ne kadar kullanıcı deneyimini geliştirse de, bazı kullanıcılar için yıkıcı ve kafa karıştırıcı da olabilir. Bu nedenle, değişiklikleri uygularken kullanıcı arayüzünü ve kullanıcı deneyimini göz önünde bulundurmak önemlidir [49].

- **Yenilenebilir enerji**

Yapay zeka destekli kestirimci bakım sistemleri, bağlı sensörler ve artırılmış gerçeklik gibi yeni teknolojiler yenilenebilir enerji kaynaklarının benimsenmesini hızlandırabilir [50] Güneş panelleri, rüzgar türbinleri veya hidroelektrik sistemlerinin işletimi ve bakımının simüle edilmesi, öğrencilerin kontrollü bir ortamda pratik beceriler kazanmasına olanak tanırken [51]. Tıpkı tarım sektöründe olduğu gibi, yeni teknolojilerin kullanımı önemli riskleri de beraberinde getirmekte, bu da dijital hijyen uygulamalarını sistemlerin korunmasında önemli bir etken haline getirmektedir[52]

Robotlar, sanal gerçeklik (VR), artırılmış gerçeklik (AR) ve simülatörler gibi yenilikçi teknolojilerin kullanımı, öğretmenlerin öğrencilerin mesleki becerilerini geliştirirken aynı zamanda dijital ve sosyal becerilerini de geliştirmelerini sağlar. Bu teknolojilerin esneklik, maliyet ve güvenlik açısından avantajları olduğu için önümüzdeki yıllarda mesleki eğitim ve öğretimde daha yaygın hale gelmesi muhtemeldir. [39] Dijital teknolojiyi güvenli, sağlıklı, sorumlu ve saygılı bir şekilde hayatımıza entegre etmek için iyi bir dijital hijyen öğretimi şarttır [9]

Ünite 4- Dijital Hijyen Kültürü İyi Uygulama Örneği:

Önceki ünitelerde, hem start-up'larda hem de Mesleki Eğitim ve Öğretim kurumlarında sağlam bir dijital hijyen kültürü geliştirmenin önemli yönlerini inceledik. Güvenli ve verimli bir dijital ortam sağlamak için dijital hijyen uygulamalarını izlemenin, gözden geçirmenin ve sürekli olarak iyileştirmenin önemini araştırdık. Bu tartışmalar, iyi bir dijital hijyen kültürü geliştirmenin rolünü vurguladı.

Şimdi, Modül 3'ün son bölümü olan Ünite 4'e adım atarken, dijital hijyen ilkelerinin pratik kullanım durumlarını sergileyen örneklerle gerçek dünya uygulamalarına dalmak üzereyiz.

Dünya Çapında Dijital Hijyen Kullanım Örnekleri

- **Dijital hijyen uygulamalarını teşvik etmek için özel bir araç seti (Sırbistan)**

İyi dijital hijyen uygulamalarının dikkate değer bir örneği, Belgrad merkezli bir vakıf olan Share Cert tarafından hazırlanan ve stratejik siber güvenlik önlemlerini vurgulayan bir rehberdir[53]. En yaygın tehditlerin ve güvenlik önlemlerinin sistematik bir şekilde kategorize edildiği bu rehber kitap, bireylerin ve kuruluşların dijital ortamdaki en acil konular hakkında bilgi sahibi olabilecekleri ve dijital hijyen kültürü hakkında genel ipuçlarına sahip olabilecekleri açık bir platform aracılığıyla desteklenmektedir.

- **Dijital Hakların korunması için Kamu Farkındalığı kampanyaları (Yunanistan)**

Dijital hakların korunması açısından bir diğer önemli girişim Yunanistan merkezli olup, özel hayatın gizliliği, kişisel verilerin korunması, dijital alanlarda ayrımcılığın yasaklanması ve bilgi edinme özgürlüğü konularına odaklanan bir sivil toplum kuruluşu (STK) olan Homo Digitalis'tir. 100'den fazla üyesiyle, kamu yararı adına çalışmalara aktif olarak katılmakta ve araştırmalar yürütmektedirler; bu da yasa koyucuların dijital haklarla ilgili konuları daha iyi anlamalarına yardımcı olabilir [54].

- **Giderek dijitalleşen sivil toplum için hızlı müdahale kiti (Küresel)**

Uluslararası Bilgisayar Acil Durum Müdahale Ekipleri (CERTs) ve Hızlı Müdahale Ağı (RaReNet) ağları, hızlı müdahale ekiplerinin, dijital güvenlik eğitmenlerinin ve teknoloji meraklısı aktivistlerin en yaygın dijital acil durum türlerine karşı kendilerini daha iyi korumalarına yardımcı olmak için çeşitli konularda rehberlik eden ve Dijital İlk Yardım Kiti olarak adlandırılan bir araçla işbirliği yapmıştır [55]. 13 dilde mevcut olan ve dışarıdan gelen katkılarla sürekli gelişen Dijital İlk Yardım Seti, internetin sorumlu ve güvenli kullanımını teşvik etmek için değerli bir kaynaktır.

- **Sivil toplum için dijital hijyen uygulamalarını takip etmeye yönelik esnek araçlar oluşturmak (Küresel)**

Dijital Dayanıklılık Merkezi, sivil toplumun güvenliğini sağlamak için dayanıklı dijital sistemler kurmayı amaçlayan ve 20'den fazla ülkede faaliyet gösteren kar amacı gütmeyen bir kuruluştur [56]. Projeleri arasında yanlış bilgilerin belirlenmesi ve raporlanması için tasarlanmış bir kitle kaynak aracı, güvenlik sorunlarının

raporlanması için dijital bir platform, dijital sistemlere yönelik tehdit ve saldırıların izlenmesi için bir görselleştirme aracı ve CiviCERT bünyesinde güçlü bir katılım ağı oluşturmayı amaçlayan bir topluluk aracı gibi hizmet ve araçların sağlanması yer almaktadır.

- **Sivil toplum için dijital hijyen uygulamalarını takip etmek üzere küresel olarak müdahale ekipleri arasında içerik alışverişini kolaylaştıran ağlar (Küresel)**

CiviCERT, SOME'leri, Bağımsız İnternet İçerik ve Hizmet Sağlayıcılarını, STK'ları ve bireyleri bir araya getiren bir ağdır. [57]. Ağın üyeleri, kendilerine bildirilen dijital güvenlik olaylarına müdahaleyi, diğer ortakların görüşlerine ihtiyaç duyulan işbirlikçi bir mekanizma içinde gerçekleştirir, koordine eder ve destekler. CiviCERT'in kendisi de iyi dijital hijyen uygulamalarına ayak uydurmakta, üyeler şifreli bir posta listesi ve Kötü Amaçlı Yazılım Bilgi Paylaşım Platformu gibi şifreli platformlar üzerinden iletişim kurarak sivil topluma yönelik yeni tehditler hakkında bilgi paylaşmakta ve acil durumlarla başa çıkmak için güvenilir ve standartlaştırılmış prosedürler sağlamak üzere şablonlar oluşturmaktadır.

- **Gelişmekte olan ülkelerde (Batı Asya ve Kuzey Afrika) dijital insan haklarının teşvik edilmesi**

SMEX, Batı Asya ve Kuzey Afrika'da dijital ortamlarda insan hakları savunuculuğu yapan bir STK'dır [58]. Dijital hijyen uygulamaları açısından, internet kullanıcılarına, aktivistlere ve insan hakları örgütlerine siber güvenlik sorunları için destek sunmakta ve genel kamuoyunu düzenlemeler ve internet hukuku hakkında bilgilendirmek için programlar oluşturmaktadır. SMEX ayrıca, dijital hijyen uygulamalarının farkındalığını ve uygulanmasını teşvik etmek için yerel ve uluslararası ortaklarla aktif olarak işbirliği yapmakta, Batı Asya ve Kuzey Afrika'da dijital alanda insan haklarını savunan bireyler ve kuruluşlar için daha güvenli bir çevrimiçi ortamı teşvik etmektedir.

- **K-12 Öğrencileri için Dijital Beceriler Müfredatı (Kuzey Amerika)**

Dijital hijyen kavramı dünya genelinde eğitim sistemlerinde giderek daha fazla önemsenmektedir. K-12 öğrencilerine özel dijital okuryazarlık materyalleri hazırlama konusunda uzmanlaşmış kuruluşlardan biri olan Common Sense Media, medya ve dijital ortamların çocukların fiziksel, duygusal, sosyal ve zihinsel ihtiyaçları üzerindeki etkisine ilişkin veriye dayalı içgörülerle öğrencileri, ebeveynleri ve öğretmenleri güçlendirmeyi amaçlayan Kuzey Amerika merkezli bağımsız bir kuruluştur [59]. Araştırma destekli Dijital Vatandaşlık Müfredatı, okullardaki önemli medya ve teknoloji konularını ele almaktadır: Zorbalıktan Nasıl Korunuruz? Mahremiyetimizi Nasıl Koruruz? ve Yanlış Bilgilere Nasıl Karşı Koyarız?

- **Daha İyi Dijital Okuryazarlık için Eğitim Materyalleri (Kuzey Amerika)**

Dijital Okuryazarlık Merkezi, açık kaynaklı materyallerin araştırılmasını ve oluşturulmasını teşvik etmeyi amaçlayan, kar amacı gütmeyen bir Amerikan kuruluşudur [60] Farklı eğitim bağlamlarında kullanılabilecek ve uyarlanabilecek müfredat tasarım araçları, dersler, etkinlikler ve değerlendirmelerin yanı sıra [61]. Medya okuryazarlığı, dijital hijyen uygulamalarının önemli bir parçasıdır ve medya okuryazarlığına yapılan vurgu

sadece dijital hijyeni geliştirmekle kalmaz, aynı zamanda dijital dünyanın karmaşıklıklarına daha iyi hazırlıklı, daha bilgili ve anlayışlı bir toplum yetiştirir.

- **Avrupa Siber Güvenlik Ayı (Avrupa)**

Her yıl Ekim ayı, Avrupa Birliği Siber Güvenlik Ajansı (ENISA) ve Avrupa Komisyonu tarafından düzenlenen önemli bir etkinlik olan Avrupa Siber Güvenlik Ayı (ECSM) olarak kutlanmaktadır [62]. AB vatandaşları ve kuruluşları arasında siber güvenlik farkındalığını güçlendirmeye adanmış olan ECSM, AB'nin iyi dijital hijyen uygulamalarını teşvik etmeye yönelik çok boyutlu yaklaşımlarından biridir. Ekim ayı boyunca konferanslar, çalıştaylar ve web seminerleri, yalnızca siber güvenlik konusunda farkındalığı arttırmakla kalmayıp aynı zamanda güncel bilgileri ve uzman tavsiyelerini aktif olarak paylaşan kapsamlı bir kampanya oluşturmaktadır. İnternetin daha güvenli kullanımını teşvik etmeyi amaçlayan ECSM, dijital hijyen ipuçları sunmakta ve CiviCERT gibi küresel ağlara ve SMEX gibi bölgesel STK'lara benzer şekilde, Avrupa Birliği genelinde iyi dijital hijyen uygulamalarının teşvik edilmesi ve sürdürülmesinde hayati bir rol oynayan kapsamlı ve işbirliğine dayalı bir çaba olarak ortaya çıkmaktadır.

- **Okul öncesi öğrencileri için siber güvenlik oyunu (Global)**

Interland [63] Google'ın "Be Internet Awesome" projesinin bir parçası olan interaktif bir oyundur. [64]genç öğrenciler arasında dijital hijyen uygulamalarını teşvik etmek için entegre bir programdır. Dinamik ve interaktif bir oyun olan Interland, oyunlaştırma yoluyla iyi dijital hijyen uygulamalarının bazı temel yönlerini öğretmek için uygulamalı bir yaklaşım sunarak oynanışıyla öğrencilerin ilgisini çekmektedir [65] KAYNAK. Gizlilik, kimlik avı, bilgisayar korsanlığı ve siber zorbalık gibi karmaşık konular, yetkinlik seviyelerine uygun renkli animasyonlarla küçük öğrencilere aktarılıyor [66] Genel olarak Interland, teknoloji kullanımı yoluyla küçük yaşlardan itibaren iyi dijital hijyen uygulamalarının aşılanması açısından kayda değer bir örnek teşkil etmektedir.

Bu modülde, iyi dijital hijyen uygulamalarının hayata geçirilmesini ve önemini ele aldık. Kurumunuzda çeşitli yönetim seviyelerinde bir dijital hijyen kültürü geliştirmek, bu uygulamaların sürekli iyileştirilmesine yönelik yöntemleri keşfetmek, gelecekte hasat edilecek fırsatlar ve üstesinden gelinmesi gereken zorluklar hakkında bilgi sahibi olmak ve ardından dünyanın dört bir yanından vaka çalışmalarını incelemek gibi konuları ele aldık.

İyi dijital hijyen uygulamaları hakkında daha fazla tavsiye ve strateji için bu rehberin diğer modüllerine göz atın ve Good Digital Hygiene for Startups web sitesini ziyaret edin.

Kaynaklar

Ünite 1 - Girişimlerde ve Mesleki Eğitim Kurumlarında Dijital Hijyen Kültürü Oluşturma

[1] Boulet, C. (2006). Dijital Hijyen: Kirli Bir Ağda Temiz Yaşam. *Arayüz: Eğitim, Toplum ve Değerler Dergisi 6(3).* Erişim adresi: Dijital Hijyen: Kirli Bir Ağda Temiz Yaşam (core.ac.uk) [Erişim Tarihi 05.12.2023]

[2] Groysberg, B., Lee, J., Price, J., & Cheng, J. Y.-J. (2018, Ocak-Şubat). Liderin kurum kültürü rehberi. *Harvard Business Review.* Erişim adresi: The Leader's Guide to Corporate Culture (hbr.org) [Erişim Tarihi 05.12.2023]

[3] Trevors, M. (2017). Siber hijyen: 11 temel uygulama. Yazılım Mühendisliği Enstitüsü Blogu. Retrieved from https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/ [Erişim Tarihi 05.12.2023]

[4] Ly, B. Dijital Dönüşümsel Liderlik, Örgütsel Çeviklik ve Dijital Dönüşümün Etkileşimi. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01377-8

[5] Harvard Business School Online. (n.d.). *Nasıl Daha Etkili Bir Lider Olunur.* Harvard Business School Yayıncılık. https://info.email.online.hbs.edu/leadership-ebook adresinden alındı.

[6] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). Dijitalleşen dünyada liderliğin rolü: Bir inceleme. *Frontiers in Psychology,* 10, 1938. https://doi.org/10.3389/fpsyg.2019.01938

[7] Cisco. (n.d.) Cisco Öğrenim Ağı Mağazası. https://learningnetworkstore.cisco.com/ adresinden alındı.

[Erişim Tarihi 06.12.2023]

[8] Avrupa Birliği Siber Güvenlik Ajansı (ENISA). (n.d.). Siber güvenlik uzmanları için çevrimiçi eğitim materyali: Teknik ve operasyonel. ENISA. https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#identification_handling adresinden alındı [Erişim Tarihi 06.12.2023]

[9] Sklar, A. (2017). Sağlam, akıllı ve güvenli: İyi dijital hijyen öğretmek için bir savunma. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Erişim Tarihi 06.12.2023]

[10] Glazer, K. (2017, 22 Mart). İyi bir dijital hijyen için hızlı bir rehber. *Şimdi Okuryazarlık*. https://www.literacyworldwide.org/blog/literacy-now/2017/03/22/a-quick-guide-to-good-digital-hygiene adresinden alındı.

[Erişim Tarihi 06.12.2023]

[11] Documenting Digital Attacks (Dijital Saldırıları Belgelemek) (n.d). Dijital İlk Yardım. https://digitalfirstaid.org/documentation/ adresinden alındı.

[12] Saraf, A. (2021, 14 Mayıs). Sağlıklı dijital hijyen için üç adım. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2021/05/14/three-steps-to-healthy-digital-hygiene/ adresinden alındı.

[Erişim Tarihi 11.12.2023]

[13] Kaspersky. (n.d.). Siber hijyen alışkanlıkları: Güvenliğinizi artırmanın 11 yolu. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits adresinden alındı.

[14] Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA). (2022). Kendinizi siber güvende tutmak için yapabileceğiniz 4 şey. Retrieved from https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe [Erişim Tarihi 11.12.2023]

[15] CHAYN. (2018). *Kendin Yap Çevrimiçi Güvenlik.* https://chayn.gitbook.io/diy-online-safety/english adresinden alındı [Erişim Tarihi 07.12.2023]

[16] Torbet, G. (2019, 3 Şubat). Sosyal medya siteleri, siz onları kullanmasanız bile davranışlarınızı tahmin edebilir. *Digital Trends.* https://www.digitaltrends.com/social-media/social-media-privacy-friends-prediction/ adresinden alındı.

[17] Toth.R., & Trifonova, T. (2021). Biri Beni İzliyor: Akıllı Telefon Kullanımı Takibi ve Tepkisellik. *Computers in Human Behavior Reports, 4*, *100142*, https://doi.org/10.1016/j.chbr.2021.100142

[Erişim Tarihi 07.12.2023]

[18] Brooks, T. (2021, 29 Temmuz). Web Tarayıcınızı Neden Güncellemelisiniz? *How-To Geek.* https://www.howtogeek.com/725165/why-you-should-update-your-web-browser/ adresinden alındı [Erişim Tarihi 08.12.2023]

[19] Barrons, M. (2016, Eylül 12). Unutmayacağınız Güvenli Parolalar Nasıl Oluşturulur. *InfoWare Group Blog.* Retrieved from https://infowaregroup.com/blog/how-to-create-secure-passwords-you-won't-forget [Erişim Tarihi 08.12.2023]

Ünite 2 - Dijital Hijyen Uygulamalarının İzlenmesi, Gözden Geçirilmesi ve Sürekli İyileştirilmesi

[20] Scott, M. (2023, 8 Aralık). Avrupa'nın Büyük Teknolojiyi ehlileştirme planı: Yeni bir yasal çerçeve. *The New York Times*. Erişim adresi: E.U. Agrees on AI Act, Landmark Regulation for Artificial Intelligence - The New York Times (nytimes.com)

[21] Rehak, D., & Grasseova, M., (2011). SWOT Analizi ile Organizasyon Bilgi Sistemlerinin Güvenliğini Değerlendirme Yolları. M. Alshawi & M. Arif (Eds.), *Kurumlarda E-Hazırlık ve Bilgi Sistemleri Yönetimi*

Vakaları: Stratejik Uyumu En Üst Düzeye Çıkarma Araçları (1. baskı, s. 162-184). IGI Global. https://doi.org/10.4018/978-1-61350-311-9

[22] Gleason, Benjamin & von Gillern, Sam. (2018). Sosyal medya ile dijital vatandaşlık: Ortaöğretimde katılımcı öğretme ve öğrenme uygulamaları. Eğitim Teknolojisi ve Toplum. 21. 200-212. https://www.researchgate.net/publication/322733013_Digital_citizenship_with_social_media_Participatory_practices_of_teaching_and_learning_in_secondary_education [Erişim Tarihi 20.12.2023]

[23] Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Bağlantılı Bir Dünyada Güvenli ve Sorumlu İnternet Kullanımı: Siber Sağlığın Teşvik Edilmesi. *Canadian Journal of Learning and Technology, 47*(4), Özel Sayı.

Ünite 3 - Dijital Hijyenin Geleceği: Zorluklar ve Fırsatlar

[24] Metz, C. (2023). Yapay Zekanın Geleceği Nedir? *The New York Times.* https://www.nytimes.com/2023/03/31/technology/ai-chatbots-benefits-dangers.html?searchResultPosition=1 adresinden alındı.

[25] Gleason, Benjamin & von Gillern, Sam. (2023). ChatGPT ile Çalışanlar Merak Ediyor: Bu İşimi Elimden Alacak mı? *The New York Times.* https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html adresinden alındı.

[26] Banholzer, M., Fletcher, B., LaBerge, L., & McClain, J. (2023, 31 Ağustos). Yenilikçi Kültüre Sahip Şirketler Üretken Yapay Zeka ile Büyük Bir Avantaja Sahip. *McKinsey & Company.* https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/companies-with-innovative-cultures-have-a-big-edge-with-generative-ai adresinden alındı [Erişim Tarihi 21.12.2023]

[27] Chng, E., Tan, A.L. & Tan, S.C. Okullarda Gelişen Teknolojilerin Kullanımının İncelenmesi: STEM Eğitiminde Yapay Zeka ve Sürükleyici Teknolojilerin Gözden Geçirilmesi. Journal for STEM Educ Res 6, 385-407 (2023). https://doi.org/10.1007/s41979-023-00092-y [Erişim Tarihi 21.12.2023]

[28] Spatharou, A., Hieronimus, S., & Jenkins, J. (2020, 10 Mart). Sağlık hizmetlerini yapay zeka ile dönüştürmek: İş gücü ve kuruluşlar üzerindeki etki. *McKinsey & Company.* https://www.mckinsey.com/industries/healthcare/our-insights/transforming-healthcare-with-ai adresinden alındı.

[29] Kopp, W., & Thomsen, B. S. (2023, 1 Mayıs). Yapay zeka öğrencilerin bütünsel gelişimini nasıl hızlandırabilir ve öğretimi nasıl daha tatmin edici hale getirebilir? *Dünya Ekonomik Forumu.*

https://www.weforum.org/agenda/2023/05/ai-accelerate-students-holistic-development-teaching-fulfilling/ adresinden alındı.

[30] Pappas, C., (2016, 7 Ocak). Öğrenme Yönetim Sistemlerini Kullanmanın En Önemli 8 Faydası. *Elearning Industry.* https://elearningindustry.com/top-8-benefits-of-using-learning-management-systems adresinden alındı.

[31] Seo, K., Tang, J., Roll, I. *ve diğerleri.* Çevrimiçi öğrenmede yapay zekanın öğrenen-eğitmen etkileşimi üzerindeki etkisi. *International Journal of Educational Technology in Higher Education* 18, 54 (2021). https://doi.org/10.1186/s41239-021-00292-9

[32] Yadav, N. R., & Deshmukh, S. S. (2023). Uluslararası Makine Zekası ve Veri Analitiği Uygulamaları Konferansı Bildirileri. *Uluslararası Makine Zekası ve Veri Analitiği Uygulamaları Konferansı Bildirileri (ICAMIDA 2022)* https://www.atlantis-press.com/article/125986295.pdf adresinden alındı.

[33] Duball, J. (2020). Çevrimiçi Öğrenime Geçiş Öğrenci Gizliliği Endişelerini Ateşliyor. *Uluslararası Gizlilik Profesyonelleri Derneği (IAPP).* https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/ adresinden alındı.

[34] Amerika Birleşik Devletleri Uluslararası Ticaret İdaresi. (n.d.). Avrupa Birliği - Veri Gizliliği ve Koruması. https://www.trade.gov/european-union-data-privacy-and-protection adresinden alındı.

[35] Gonzalez, G. (2018, 10 Ekim). Amazon, Kadınlara Karşı Önyargı Gösteren Yapay Zeka İşe Alım Aracını Terk Etti. *Inc.* https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html adresinden alındı.

[36] Gatzemeier, S. (2021, 18 Haziran). Yapay Zeka Önyargısı: Nereden Geliyor ve Bu Konuda Ne Yapabiliriz? *UC Berkeley Bilgi Okulu Blogu.* https://blogs.ischool.berkeley.edu/w231/2021/06/18/ai-bias-where-does-it-come-from-and-what-can-we-do-about-it/ adresinden alındı.

[37] Akgun, S., Greenhow, C. Eğitimde yapay zeka: K-12 ortamlarında etik zorlukların ele alınması. *AI Ethics* 2, 431-440 (2022). https://doi.org/10.1007/s43681-021-00096-7 adresinden alındı.

[38] Polluveer, K. (2023). İnovasyon Politikası. *Avrupa Parlamentosu Bilgi Notu.* https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.6.pdf adresinden alındı.

[39] OECD (2021), Mesleki Eğitim ve Öğretimde Öğretmenler ve Liderler, OECD Mesleki Eğitim ve Öğretim İncelemeleri, OECD Yayıncılık, Paris, https://doi.org/10.1787/59d4fbb1-en

4. Mesleki eğitim ve öğretimde yenilikçi pedagojik yaklaşımların teşvik edilmesi | Mesleki Eğitim ve Öğretimde Öğretmenler ve Liderler | OECD iLibrary (OECD-ilibrary.org)

[40] eduLAB Pty Ltd. (2020, 12 Ağustos). eduLAB Tanıtım Videosu. *Vimeo.* https://vimeo.com/447337687 adresinden alındı.

[41] N.d. (2022, 27 Mart). 2022 ve Sonrasında Siber Güvenliği Etkileyecek 7 Teknoloji İnovasyonu. *Cloud Security Alliance Blog.* Retrieved from 2022'de Siber Güvenliği Etkileyecek 7 Teknoloji İnovasyonu | CSA (cloudsecurityalliance.org)

[42] Dünya Ekonomik Forumu. (2021, Mart). Tarımsal İnovasyon için Yapay Zeka. *Topluluk Belgesi.* WEF_Artificial_Intelligence_for_Agriculture_Innovation_2021.pdf adresinden alındı (weforum.org)

[43] BIS Araştırma. (2021, 7 Ekim). Tarımda Artırılmış Gerçekliğin (AR) Giderek Daha Fazla Benimsenmesi. https://blog.marketresearch.com/the-increasing-adoption-of-augmented-reality-ar-in-agriculture adresinden alındı.

[44] BIS Araştırma. (2021, 7 Ekim). Tarımda Artırılmış Gerçekliğin (AR) Giderek Daha Fazla Benimsenmesi. https://eos.com/blog/smart-farming/ adresinden alındı.

[45] Tzachor, A., Devare, M., King, B. ve diğerleri (2022). Tarımda sorumlu yapay zeka, risklerin ve dışsallıkların sistemik bir şekilde anlaşılmasını gerektirir. *Nature Machine Intelligence, 4*, 104-109. https://doi.org/10.1038/s42256-022-00440-4

[46] Bettencourt, J. (2023, 16 Kasım). Konaklama endüstrisi misafir deneyimi için AR ve VR'yi nasıl kullanıyor? *Otel Yönetimi.* https://www.hotelmanagement.net/tech/how-hospitality-industry-using-ar-vr-guest-experience adresinden alındı.

[47] Kover, A. (2020, 10 Mart). Misafirperverliğe yeni bir bakış açısı: Hilton empati öğretmek için sanal gerçekliği nasıl kullanıyor? *Facebook Reality Labs Tech Blog.* https://tech.facebook.com/reality-labs/2020/3/a-new-perspective-on-hospitality-how-hilton-uses-vr-to-teach-empathy/ adresinden alındı.

[48] Guenther, D. (2021, 9 Eylül). Sanal Gerçeklik eğitimi, konaklama sektörü çalışanlarını bir sonraki seyahat çağına hazırlıyor. *Medium.* Retrieved from https://medium.com/@DanielGuenther/virtual-reality-training-prepares-hospitality-workers-for-the-next-era-of-travel-7a8d5d3b8be5

[49] Pencarelli, T. Seyahat ve turizm endüstrisinde dijital devrim. *Inf Technol Tourism* 22, 455-476 (2020). https://doi.org/10.1007/s40558-019-00160-3 adresinden alındı.

[50] Amon, C., Slaughter, A., & Motyka, M. (2018, Eylül). Küresel yenilenebilir enerji trendleri. *Deloitte.* https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/global-renewable-energy-trends.html adresinden alındı.

[51] Travelers. (n.d.). Güneş ve Rüzgar Enerjisi Tesislerinde Kestirimci Bakım. https://www.travelers.com/resources/business-industries/energy/predictive-maintenance-at-solar-and-wind-installations adresinden alınmıştır.

[52] Victor, D. G. (2019, 10 Ocak). Yapay zeka enerji ve iklimin geleceğini nasıl etkileyecek? *Brookings Enstitüsü.* https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/ adresinden alındı.

[9] Sklar, A. (2017). Sağlam, akıllı ve güvenli: İyi dijital hijyeni öğretmek için bir savunma. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Erişim Tarihi 06.12.2023]

ÜNİTE 4 - Dijital Hijyen Kültürü İyi Uygulama Kullanım Örneği:

[53] ShareCert Toolkit. (n.d.). Cybersecurity Toolkit adresinden alındı

[54] Homo Digitalis. (2022, 13 Temmuz). Homo Digitalis için büyük bir başarı: Yunanistan DPA'sı CLEARVIEW AI'ye 20 milyon € ceza verdi. https://homodigitalis.gr/en/posts/12155/ adresinden alındı.

[55] Dijital İlk Yardım. (n.d.). Digital First Aid Kit adresinden alındı

[56] Digiresilience. (n.d.). Center for Digital Resilience adresinden alındı

[57] CivicERT. (n.d.). CiviCERT adresinden alındı

[58] SMEX. (n.d.). SMEX'ten alındı

[59] Common Sense Media. (n.d.). Dijital Okuryazarlık ve Vatandaşlık. https://www.commonsensemedia.org/what-we-stand-for/digital-literacy-and-citizenship adresinden alındı.

[60] Medya Okuryazarlığı Merkezi. (2005). Medya Okuryazarlığının Beş Temel Sorusu. https://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf adresinden alındı.

[61] Medya Okuryazarlığı Merkezi. (n.d.). https://www.medialit.org/https://www.medialit.org/ adresinden alındı.

[62] Avrupa Siber Güvenlik Ayı. (n.d.). https://cybersecuritymonth.eu/ adresinden alındı.

[63] Google. (2023). Be Internet Awesome: Interland. https://beinternetawesome.withgoogle.com/en_us/interland/ adresinden alındı.

[64] Google. (2023). Be Internet Awesome: Interland. https://beinternetawesome.withgoogle.com/en_us adresinden alındı.

[65] Bogardus Cortez, M. (2018, 17 Nisan). Dijital Vatandaşlık Müfredatı: Dijital Okuryazarlık, Siber Hijyen ve Daha Fazlası. *EdTech Magazine.* How to Design Your Digital Citizenship Curriculum - EdTech (edtechmagazine.com) adresinden alındı.

[66] Bogardus Cortez, M. (2014, 24 Temmuz). Google ve ITSE'den Dijital Vatandaşlık Oyunu Eğitmeyi Amaçlıyor. *EdTech Magazine.* Google & ITSE'nin Dijital Vatandaşlık Oyunu Eğitmeyi Amaçlıyor | EdTech Magazine adresinden alındı

[12*] Durbin, S. (2019). 2020'nin en büyük 3 küresel siber güvenlik tehdidi. *Dark Reading.* Retrieved from https://www.darkreading.com/vulnerabilities-threats/crystal-ball-the-top-3-global-cybersecurity-threats-for-2020 [Erişim Tarihi 06.12.2023]

[13*] Ponemon, L., & Beri, S. (2014). *Veri İhlali: Bulut Çarpan Etkisi.* Retrieved from **https://www.slideshare.net/Netskope/data-breach-the-cloud-multiplier-effect** [Erişim Tarihi 06.12.2023]

[14*] Hadlington, L. (2017). Siber güvenlikte insan faktörleri: İnternet bağımlılığı, dürtüsellik, siber güvenliğe yönelik tutumlar ve riskli siber güvenlik davranışları arasındaki bağlantının incelenmesi. *Heliyon,* 3. **https://doi.org/10.1016/j.heliyon.2017.e00346**

[15*] Telefonica Tech. (2022, 10 Kasım). Siber Güvenlikte İnsan Faktörleri: Kendinizi Koruyun. *Telefonica Tech Blog.* **https://telefonicatech.com/en/blog/human-factors-in-cybersecurity** adresinden alındı [Erişim Tarihi 11.12.2023]

[XXXXX] Irwin, L. (2020, Haziran). *Kimlik avı e-postasını tespit etmenin 5 yolu - örneklerle*. ITGovernance. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email [Erişim Tarihi 08.12.2023]

[XXXXXXX] Federal Ticaret Komisyonu Tüketici Bilgileri (2019, Mayıs). *Kimlik Avı Dolandırıcılığı Nasıl Tanınır ve Önlenir.* https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [Erişim Tarihi 08.12.2023]

[XX] DCAF (Cenevre Güvenlik Sektörü Yönetişimi Merkezi), Babić, V., & Bratić, A. (2022, Ekim). *Çevrimiçi Güvende Kalma Kılavuzu: Kamu Kurumları ve KOBİ'ler için Siber Hijyen.* **https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf** adresinden alındı [Erişim Tarihi 06.12.2023]