Co-funded by the Erasmus+ Programme of the European Union

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Ünite 1 Hafta 1** **Ünite adı: Giriş Web Semineri**	
Öğrenme Aktiviteleri	❑ **Web Semineri** ❑ **Alıştırmaları** ❑ **Atölye Sunumu** ❑ **Diğer**
Öğrenme Sorumlusu	• Gabriel Vladut • Valentin Istratie
Öğrenme Etkinliği Hedefleri	1. Erasmus+ InCyT projesi hakkında giriş 2. Hedef 3. Sonuçlar ve ürünler 4. Kendinizi siber saldırılara karşı nasıl korursunuz? 5. Eğitim ve mentorluk 6. Sosyal mühendislik 7. Sosyal Ağ (Sosyal Medya)
Kazanılacak Beceriler	• TS3 Ağ Güvenliği • TS4 Penetrasyon (istismar edilebilir güvenlik açıkları) testi • SS3 Bilişsel ve davranış analizi
Öğrenme aktivitesinin süresi	2 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • Erasmus+ InCyT projesi / hedefleri / Sonuçları ve ürünleri hakkında bilgi edinmek • Kendinizi siber saldırılara karşı nasıl korursunuz? • Eğitim ve mentorluk • Sosyal mühendislik / Sosyal Ağ (Sosyal Medya)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Modül hakkında kısa bilgi

Giriş
InCyT, mesleki eğitim ve öğretim kurumlarının siber saldırılardan kaçınmak için profesyoneller için değil, profesyoneller için siber güvenlikte gerekli olan yetkinlikleri ve becerileri tanımlamaları için bir mekanizma sağlayan bir Çerçeve, bir eğitim metodolojisi oluşturmayı amaçlayan bir Erasmus + projesidir. dijital boşluklar ve diğerleri. NIST'in Ulusal Siber Güvenlik Eğitimi Girişimi (NICE), "siber güvenlik çalışmaları için gerekli görevleri yerine getirecek bilgi, beceri ve yeteneklere sahip kişilerin" eksikliğini gidermek için çok önemli bir adım atılması gerektiğinin altını çiziyor. Böyle bir işgücü, "bilgili ve deneyimli insanlarla çalışan teknik ve teknik olmayan rolleri" içerecektir. Proje bu bağlamda bazı çözümleri uygulamak isteyecektir. Öncelikle mesleki eğitim ve şirketlerin siber saldırılardan kaçınmak ve bu durumu iyileştirmelerine yardımcı olmak için profesyoneller için değil, profesyoneller için siber güvenlikte gerekli olan dijital boşlukları ve diğer boşlukları tanımlamaları için bir mekanizma sağlayan bir Çerçeve geliştirmeyi hedeflemektedir. Disiplinlerarası eğitim ve mentorluk programlarının özellikle siber güvenlik alanındaki avantajları göz önünde bulundurularak proje, KOBİ'ler için e-mentorluk destekli dijital disiplinlerarası eğitim programlarını test ederek mesleki eğitime uyarlayacaktır. Eğitimciler, araştırmacılar ve bilgi teknolojilerini kullanan kişiler arasında işbirliği ve iletişim gereklidir. Bir sorun, şirketlerin, özellikle de daha az kaynağa sahip KOBİ'lerin, çalışanlarının yetkinlik ve beceri boşluklarını, mevcut durumu değerlendirme yöntemlerini ve çalışanlarını yeniden vasıflandırmak için eğitim olanaklarını kullanma yöntemlerini takdir etmek için yardıma ihtiyaç duymalarıdır. Öğrenciler, ilgili metni okuyarak, akış web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek bu yönler hakkında bilgilendirilebilirler. Tüm bu dokümanlar dijital interaktif proje platformundadır. Öğrenciler cevaplarını öz değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalarla ilgili cevaplar ilgili tartışma forumuna kaydedilmeli ve haftada bir kez ortak organize toplantıda mentorla tartışılmalıdır. Öğrenci, özellikle toplantılar sırasında diğerleriyle işbirliği içinde çalışabilir ve mentorluk yapabilir. Eğitimin yansıtılması ve değerlendirilmesi için önemli olan e-portfolyo geliştirmeleri desteklenecektir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

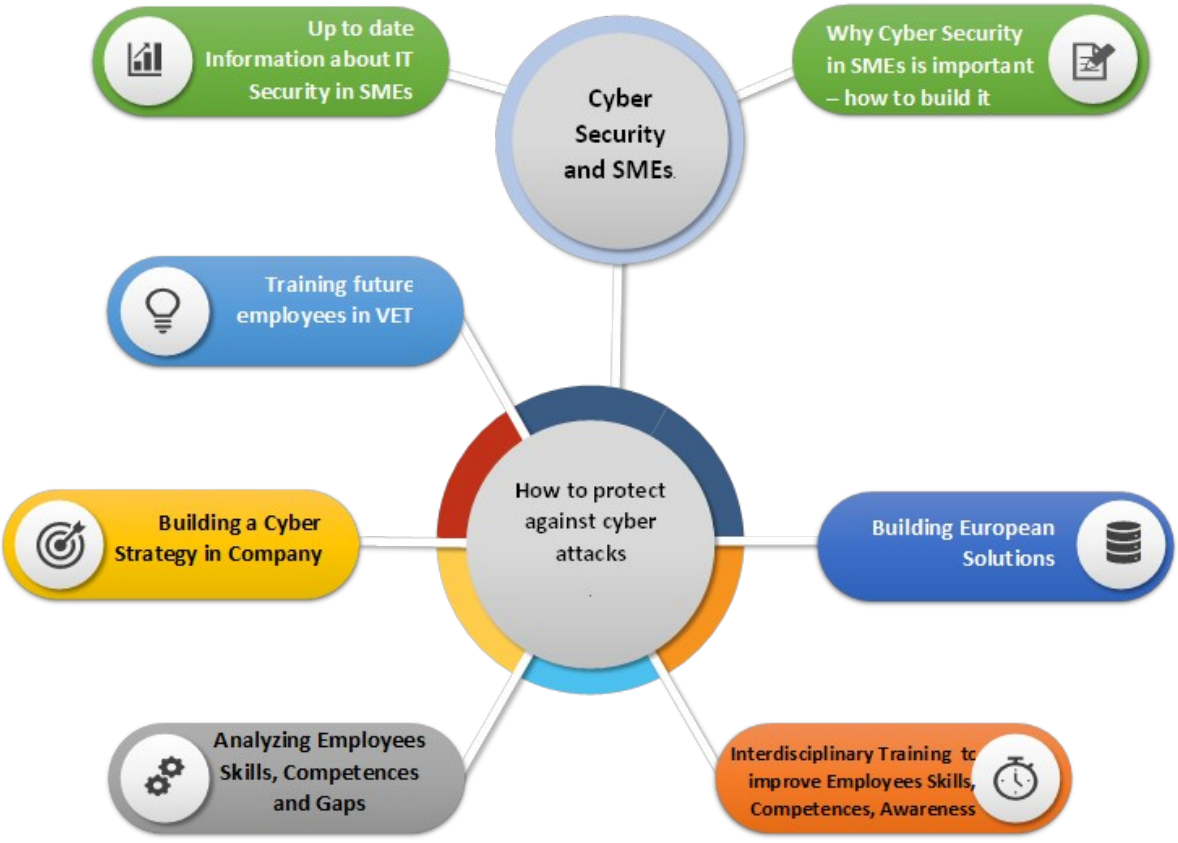
Co-funded by the Erasmus+ Programme of the European Union

Öğrenme Materyalinin İçeriği

Yetkinlik Çerçevesi

Projemizde 3 ulusötesi toplantı olacak. Projenin 3., 13. ve 20. aylarında planlanmıştır. 24 aylık bir projeyi yürütmek için 3 toplantının yeterli olmayacağını düşündüğümüz için bazı ek proje toplantıları yapılacaktır. Bu toplantılar çevrimiçidir ve her ay düzenli olarak yapılır. Proje üst yönetim ekibi bu projeleri organize edecektir.

Projeler, proje koordinatörü, WP lideri tarafından yönetilecektir. Projemizde 7 çarpan etkinliği olacak. Her ortak kurum, proje fikrini kendi ülkesinde yaygınlaştırmak ve geliştirilen ürünleri paylaşmak için bu etkinlikleri düzenleyecektir. Her ortak kurum, KOBİ çalışanları ve öğretmenleri için Siber Güvenlik alanında Disiplinlerarası Eğitim düzenleyecek.



Şekil 1: InCyT projesi tarafından desteklenen faaliyetler

Hedef

InCyT projesi bazı çözümleri uygulamak isteyecektir:

- Mesleki eğitim ve şirketlere, siber saldırılardan kaçınmak için profesyoneller için değil,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

profesyoneller için siber güvenlikte gerekli olan yetkinlik ve becerileri tanımlamaları için bir mekanizma sağlayan bir Çerçevenin geliştirilmesi, dijital boşluklar ve diğerleri.

- Disiplinlerarası eğitim ve mentorluk programlarının özellikle siber güvenlik alanındaki avantajları göz önünde bulundurularak projenin geliştireceği ve test edeceği dijital disiplinlerarası eğitim programları desteklenerek KOBİ'ler için işbirlikçi bir e-Öğrenme platformu
- Veteriner için uyarlayın.
- Bir Avrupa aktarılabilirlik modeli geliştirmek
- Disiplinlerarası eğitim ve mentorluk programlarının özellikle siber güvenlik alanındaki avantajları göz önünde bulundurularak proje, KOBİ'ler için e-mentorluk destekli dijital disiplinlerarası eğitim programlarını test ederek mesleki eğitime uyarlayacaktır.

Projenin çıktıları :

- Uygulama için Metodolojik Çerçeve
- Mevcut ve takip edilen eğitim (kurslar)
- Disiplinlerarasılık ve mentorluk kullanarak bunların iyileştirilmesi için fırsatlar.
- Öğrenme ve mentorluk metodolojisi

Ürünler:

1. Çerçeve

2. KOBİ'ler için mentorluk ile desteklenen dijital bir Disiplinlerarası siber güvenlik eğitim materyali ve mesleki eğitim özel kursu için uyarlanmış bir metodoloji.

3. Eğitimi destekleyen dijital bir platform

4. Disiplinlerarası becerilerin KOBİ ve KDV için nasıl avantajlar sağladığını raporlayın.

5. Test edilmiş disiplinlerarası eğitim ve mentorluk için Avrupa aktarılabilirlik modeli

Ortaklar : Almanya (koordinatör), Türkiye, Polonya, İtalya, Avusturya, Danimarka, Romanya.

Faaliyetleri

- Siber Güvenlik Metodolojik Çerçevesi - Önde Gelen Kuruluşlar: IAT, Almanya, İtalya
- Dijital Disiplinlerarası Siber Güvenlik Eğitim Materyali - Lider Kuruluş: St. Pölten Uygulamalı Bilimler Üniversitesi, Avusturya
- Siber Güvenlik için BİT Platformu - Lider Kuruluş: IPA, Romanya
- Siber Güvenlik için Metodolojik Model - Lider Kuruluş: Politechnik Üniversitesi, Polonya

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Aktarılabilirlik Modeli - Lider Kuruluş: Avrupa Eğitim Merkezi Kopenhag, Danimarka
- Çarpan Etkinlikleri - Lider Kuruluş: Türkiye

Kendinizi siber saldırılara karşı nasıl korursunuz?

Dijital ekonomi öncelikle verilere dayanmaktadır. Endüstri 4.0, siber-fiziksel sistemler ve Nesnelerin İnterneti çağında, giderek daha fazla ürün ve süreç dijitalleştirilmektedir. Bu verilerin ve ilgili bilgi işlem sistemlerinin korunması anlamına gelen siber güvenlik, bugün ekonomik tarihin herhangi bir zamanından daha önemlidir.

İş süreçleri önemli ölçüde kesintiye uğrayabilir, yavaşlayabilir veya hatta tamamen engellenebilir, örneğin veri kayıtları yanlış, eksik veya hiç mevcut değilse, sistemler arasındaki veri senkronizasyonu bozulursa, BT sistemleri yanlış çalışır veya tamamen başarısız olursa.

Özellikle KOBİ'ler bu konularla ilgili suç faaliyetlerinin hedefidir. Büyük şirketlerin aksine, kaynakları sınırlıdır - ve bilgisayar korsanları bunu bilir! KOBİ'ler Avrupa ekonomisinin bel kemiğidir, yani Almanya'daki şirketlerin %99'undan fazlası KOBİ'dir.

İşgücünün yarısından fazlası KOBİ'ler tarafından istihdam edilmektedir. Bu nedenle KOBİ'lerin siber saldırılardan kaçınmasına yardımcı olmak gerekiyor.

Siber Güvenlik Eğitim Girişimi, "siber güvenlik çalışmaları için gerekli görevleri yerine getirecek bilgi, beceri ve yeteneklere sahip bireylerin" eksikliğini gidermek için kritik bir adım atılması gerektiğine işaret ediyor.

Böyle bir grup, "bilgi ve deneyime sahip çalışanlar tarafından doldurulan teknik ve teknik olmayan işlevleri" içerir.

Ancak gerekli disiplinler arası becerilere sahip bir iş gücü oluşturmak ve eğitimciler, araştırmacılar ve bilişim teknolojilerini kullanan kişiler arasındaki iletişim sorununu çözmek zordur.

Bu gruplar arasında işbirliği ve iletişim gereklidir.

Bir sorun, şirketlerin, özellikle de daha az kaynağa sahip KOBİ'lerin, çalışanlarının becerilerini ve boşluklarını değerlendirmek, mevcut durumu iyileştirmek için dijital yöntemler kullanmak ve çalışanlarını yeniden vasıflandırmak için eğitim fırsatları düzenlemek için yardıma ihtiyaç duymalarıdır.

Eğitim ve mentorluk

Gelecektekiler de dahil olmak üzere girişimciler, karmaşık düşünme biçimlerine ve disiplinlerarası öğrenme gerektiren farklı sektörlerden gelen bilgileri anlama ve entegre etme yeteneğine ihtiyaç

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

duyarlar.

Karmaşık mühendislik problemleri, neredeyse doğal bir şekilde disiplinlerarası bir durum yaratmayı gerektirir.

Disiplinlerarası bir yaklaşımda, öğrenciler farklı disiplinlerden ve alanlardan gelen bilgileri bütünleştirmelidir.

Disiplinlerarası bir anlayış geliştirirler, uzmanlık alanlarını ve disipline özgü düşünme biçimlerini bütünleştirmeyi öğrenirler.

Bu, bilişsel becerileri ve eleştirel düşünmeyi tek bir disiplin aracından daha fazla arttırır.

Sosyal mühendislik

- saldırganın ilgisini çeken verilere, belgelere ve bilgilere erişmek için insanları manipüle etmek (genellikle psikolojik yöntemler kullanarak) anlamına gelir.
- günümüzde bilgi güvenliğine yönelik ana tehditlerden biridir ve etkili bir siber suç biçimidir.
- veri ihlalleri gibi tehlikeli yankıları olabilir, diğer saldırı türlerinden daha fazla.
- saldırıların finansal bir amacı var ve bu nedenle örgütler önemli miktarda para kaybetti.
- özellikle tehlikelidir, çünkü yazılım ve işletim sistemlerindeki güvenlik açıklarından çok insan hatasına dayanır.

Şirketler:

- üretkenlik kaybına, çalışanların moralinde bir düşüşe ve iyileşmede zorluklara maruz kalabilirler.
- itibar hasarı var, çünkü müşteriler kuruluşun kendisini koruyabileceğine ikna olmuş değiller.
- genellikle eski bir olay yanıtını tetiklemeniz gerekir.
- gelecekteki saldırıları önlemeye yardımcı olmak için güvenlik yazılımı sağlamalıdır.
- genellikle çalışanları saldırılara hazır olmaları için yeniden eğitmek zorunda kalacaklardı.

Sosyal Mühendislik Eğitimi (siber farkındalık)

- Sosyal mühendislik saldırılarını tanımanın önemli olduğu çalışanların ve yöneticilerin kurban olma riski yüksektir.
- toplumsal, bireysel ve vatandaş güvenliği farkındalık programlarına dahil edilebilir ve bireyleri ve kuruluşlarını koruyabilir.
- özellikle daha az kaynağa sahip KOBİ'lerde eksiktir, bu nedenle siber farkındalık eğitimini ciddiye almalarına ve çalışanların bunu almaları için fırsatlar sağlamalarına yardımcı

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

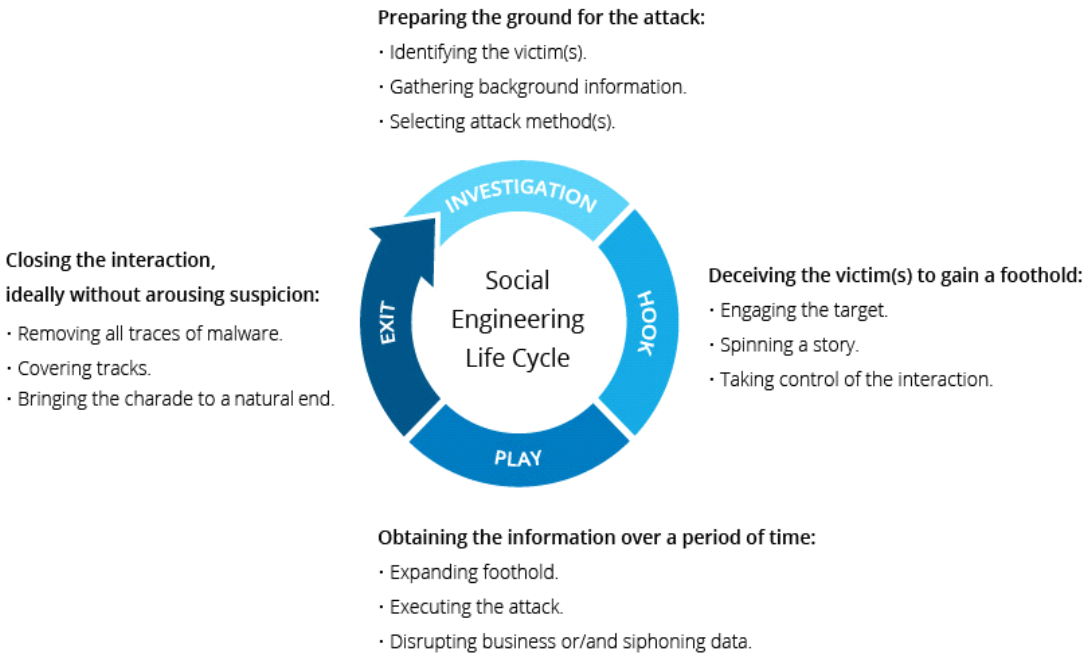
olunmalıdır.

Sosyal Mühendislik Saldırısı Yaşam Döngüsü

Saldırgan:

- İlk olarak, saldırı için gerekli olan giriş noktaları ve zayıf güvenlik protokolleri gibi gerekli temel bilgileri toplamak için hedeflenen kurbanı araştırın.
- daha sonra deneyin, kurbanın güvenini kazanın ve hassas bilgi haline gelmek veya kritik kaynaklara erişim izni vermek gibi genellikle güvenlik uygulamaları olmayan eylemler için teşvikler sağlayın.

Şekil 2 , bir saldırının yaşam döngüsünü açıklamaktadır.



Şekil 2: Bir saldırının yaşam döngüsü

Sosyal ağ

- Son yıllarda çok popüler hale geldi ve kullanıcılara aileleri, arkadaşları ve meslektaşları ile

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

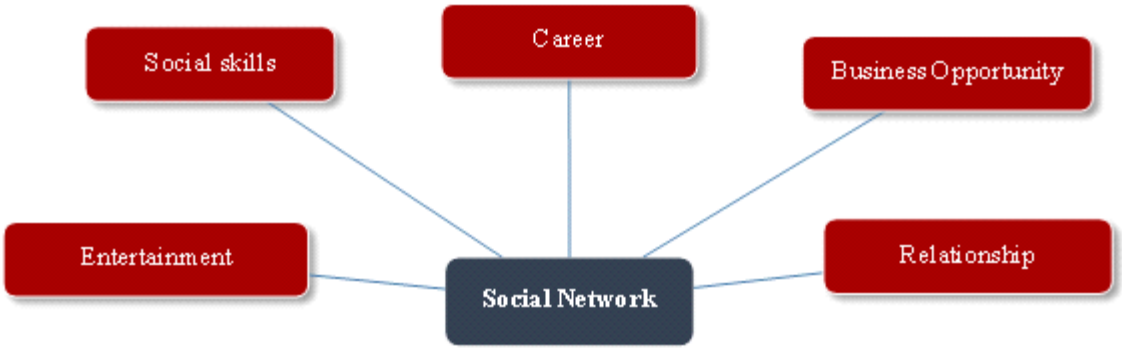
Co-funded by the Erasmus+ Programme of the European Union

iletişim kurmak için bir platform sağladı.

- ve Sosyal Ağ, arkadaşlarınızla, ailenizle, iş arkadaşlarınızla, müşterilerinizle veya müşterilerinizle bağlantı kurmak ve iletişim kurmak için İnternet tabanlı sosyal ağ sitelerinin kullanımını ifade eder.
- sunucularını İnternet'in ana ağ erişim noktalarıyla birlikte bulunan veri merkezlerinde bulundururlar.

Sosyal Medya Rolleri (Şekil 3), sosyal medyanın rol oynadığı bazı alanları göstermektedir:

- Eğlence
- İş fırsatları oluşturmak
- Kariyer yapmak
- Sosyal becerilerin geliştirilmesi
- Diğer bireylerle ilişkiler geliştirmek



Şekil 3: Sosyal Ağdaki Roller

Sosyal ağ:

- Marka bilinirliğini artırmak, marka sadakatini artırmak, dönüşüm oranlarını iyileştirmek, yeni, yeni ve eski müşterilerle erişim ve etkileşim sağlamak için müşteri arayan pazarlamacılar için bir temeldir.
- Sosyal ağlarda blog yayınları, resimler, videolar veya yorumlar paylaşarak, daha fazla insanın şirketin web sitesini ziyaret etmesini ve müşteri olmasını mümkün kılmak.
- Değişikliklere ayak uydurmayı zorlaştırır ve aynı zamanda bir şirketin pazarlama başarı oranını da etkiler.

Amerika Birleşik Devletleri ve Avrupa'daki en popüler sosyal ağ (sosyal medya) siteleri şunlardır:

- Facebook
- Instagram

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Twitter
- YouTube
- WhatsApp
- LinkedIn, profesyonelleri iş arkadaşlarıyla, iş bağlantılarıyla ve işverenlerle buluşturmaya yardımcı olur.

Sosyal ağ, insanların ve işletmelerin birbirleriyle bağlantı kurmasına, ilişkiler geliştirmesine, bilgi, fikir ve mesaj paylaşmasına olanak tanıyan teknoloji ve sosyal ağ sitelerini (Sosyal Medya) kullanarak kişisel ve iş ilişkileri geliştirmeye ve sürdürmeye dayanır.

Aile üyeleri, Facebook gibi kişisel sosyal ağlar aracılığıyla bağlantıda kalabilir, fotoğraf paylaşabilir ve yaşamları hakkında başka mesajlar gönderebilir.

İnsanlar aynı ilgi alanlarını paylaşan başkalarıyla (yabancılarla) da bağlantı kurabilirler.

Yanlış bilginin yayılması ve sosyal medya profillerini kullanmanın ve sürdürmenin yüksek maliyeti de dahil olmak üzere sosyal medyanın dezavantajları da vardır.

Sosyal platformların işlevselliği şu şekilde sınıflandırılabilir:

Ağ işlevleri, sanal platformlardaki kullanıcılar arasındaki sosyal ilişkileri geliştirmeye ve sosyal ağ grafiğini oluşturmak ve sürdürmek için işlevsellik sağlamaya hizmet eder.

Veri işlevleri, kullanıcı tarafından sağlanan içeriği ve kullanıcılar arasındaki iletişimi yönetmekten, kullanıcı etkileşimini iyileştirmeye (genişletmeye) ve platformu daha çekici hale getirmeye yardımcı olmaktan sorumludur.

Erişim kontrolü özellikleri, kullanıcı tanımlı gizlilik önlemlerini uygulamayı ve kullanıcı tarafından sağlanan veri ve bilgilere yetkisiz erişimi kısıtlamayı amaçlamaktadır.

Sosyal ağların avantajları ve dezavantajları

Faydaları

- Sosyal medya, işletmelerin şunları yapmasına olanak tanır:
- Yeni ve mevcut müşterilerle bağlantı kurmak.
- Marka bilinirliği yaratabilmek, tanıtabilmek ve artırabilmek.
- Marka satışlarını ve daha yüksek arama motoru sıralamalarını artırmak için müşterileri tarafından yapılan incelemelere ve yorumlara güvenmek.
- Yeni bir marka oluşturabilmek. Müşterilerine yüksek düzeyde hizmet göstermek.
- Ürünleri ve tüketicilerle ilişkileri geliştirebilmek.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Dezavantaj

- Yanlış bilginin yayılmasına katkıda bulunabilirler.
- Şirketler üzerinde olumsuz bir etkisi olabilir, çünkü bir markanın eleştirisi sosyal medyada çok hızlı bir şekilde yayılmıştır.
- Bir şirket profili oluşturmak ve sürdürmek için her hafta çalışma saatleri ve maliyetleri gerektirir.

Sosyal ağlarda güvenlik ve gizlilik

- Sosyal ağlarda ve medyada paylaşılan bilgiler çok hızlı bir şekilde yayılır ve bu da saldırganların bunu kazanmasını cazip hale getirir.
- Bir kullanıcı fotoğraf, video ve ses gibi kişisel içerik yüklerken kullanıcı tarafından paylaşılan bilgilerle ilgili güvenlik ve gizlilik sorunlarına saygı gösterilmelidir, çünkü saldırgan paylaşılan bilgileri kötü amaçlarla meşru olmayan amaçlarla kullanabilir.
- Güvenlik ve gizlilik konusunda kullanıcı farkındalığının olmaması, sosyal medya aracılığıyla çeşitli siber saldırılara yol açma potansiyeline sahiptir.

Tehditler üç kategoriye ayrılabilir:

- Geleneksel tehditler, kullanıcıların sosyal ağın başlangıcından bu yana karşılaştıkları tehditleri içerir.
- Modern tehditler, kullanıcı hesaplarının güvenliğini aşmak için gelişmiş teknikler kullanan saldırılardır.
- Hedefli saldırılar, herhangi bir kullanıcı tarafından çeşitli kişisel kan davaları için işlenebilen belirli bir kullanıcıyı hedef alan saldırılardır.

Sosyal ağ operatörleri için çözümler

- CAPTCHA, çok faktörlü kimlik doğrulama ve arkadaşların fotoğrafla tanımlanması gibi kimlik doğrulama prosedürleri önerilmiştir.
- Müşterinin yabancılar veya uygulamalar tarafından istenmeyen erişimden kişisel bilgilerini girmesine izin veren güvenlik ve gizlilik ayarı.

Kullanıcı, ağındaki herhangi bir kullanıcı tarafından gerçekleştirilen her türlü kötüye kullanım veya politika ihlaline ilişkin bildirim bildirir. yani, Facebook bir kullanıcı şikayeti aldığında, Facebook'un topluluk standartlarına göre incelenir ve kaldırılır.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Soru:

Sorular Tartışma Forumu kısa bir açıklama ile cevaplandırılacaktır. Mentorluk oturumları sırasında cevaplar mentor ile tartışılacaktır.

1. Cadı InCyT projesi ile ilgili beklentileriniz nelerdir?
2. Kendinizi siber saldırılara karşı nasıl korursunuz?
3. Sosyal mühendislik nedir?
4. Sosyal Ağ (Sosyal Medya) nedir?

Öz değerlendirme soruları. Cevapladıktan sonra öğrenci sonuçları görebilir ve bunları platformda kayıtlı olanlarla karşılaştırabilir

- Kendinizi siber saldırılara karşı nasıl korursunuz?
- Sosyal mühendislik nedir
- Sosyal Ağ (Sosyal Medya)

Ekleri

PowerPoint sunumu
Video filmler

Başvuru:

- InCyT – Disiplinlerarası Siber Eğitim
- Siber Olay Kurtarma
- Siber Saldırıları En Aza İndirin - Siber Dayanıklılık Stratejisi
- Siber Saldırılar Nasıl Önlenir: Kendinizi Korumanın En İyi Yolları
- Sosyal Medya Güvenliği: Bilgileriniz Ne Kadar Güvenli?
- Bilgi Sistemleri Üzerindeki İç Kontroller
- Sosyal Medyanın Benimsenmesi Yeni Riskler Getiriyor
- Sosyal Medya Güvenliği - 5 Güvenlik İpucu
- 19 Sosyal Medya Güvenliği En İyi Uygulamaları

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.