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

InCyT Eğitim Modülleri

Yöneticiler için Bilgi Güvenliği Ünite (Modül) no: (2)-Hafta:3 Birim (Modül) adı: Bilgi güvenliği yönetimi -1	
Öğrenme Aktiviteleri	❑**Web semineri** ❑**Alıştırmalar** ❑**Çalıştay** ❑**Sunum** ❑**Diğer** Streaming Webinar, Metin, Öz Değerlendirme Alıştırmaları, Tartışma forumlarında cevapları olan alıştırmalar ve eğitmen / mentor ile tartışılacak
Öğrenme Sorumlusu	• Fatma Gökdemir • Ali Gökdemir
Öğrenme Etkinliği Hedefleri	1. Bilgi güvenliği 2. Bilgi güvenliği politikaları 3. Bilgirmation security roles
Kazanılacak Beceriler	• IS 1 • IS 3 • MS 3
Öğrenme aktivitesinin süresi	2 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • Orta düzey bilgisayar becerileri

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

Bilgi güvenliği, her kuruluşun sürekliliğinin sağlanmasında büyük önem taşımakta ve elektronik ortamlar başta olmak üzere çeşitli ortamlarda kuruluşun kritik bilgilerinin ve diğer bilgi varlıklarının korunmasını sağlamaktadır. Sadece büyük şirketler, holdingler değil, aynı zamanda KOBİ'ler, devlet kurumları, kar amacı gütmeyen herhangi bir kuruluş, okul veya tek başına insanlar, farklı seviyelerde de olsa sürekli olarak bilgi güvenliği sorunları ve riskleri yaşamaktadır. Bu riskleri karşılamak için yapılan yatırımlarda, en pahalı ve en karmaşık çözüm her zaman en güvenli çözüm değildir. Her kişi veya kuruluşun en uygun ve doğru çözümü seçmesi ve uygulaması gerekir. Unutulmamalıdır ki basit ve düşük maliyetli bir güvenlik çözümü bazı kurumlar için yetersiz kalırken, aynı çözüm başka bir kurum için de yeterli ve etkili olabilir. Ancak bilgi güvenliği başlatılacak ve bitirilecek bir iş değildir. Bilgi güvenliği yönetimi, kurumlar ve bilgiler var olduğu sürece sürekli yönetilmesi ve denetlenmesi gereken bir yaşam döngüsüdür.
Bu modülde bilgi güvenliği kavramı, önemi ve bilgi güvenliği için yapılması gerekenler anlatılacaktır. Konu pratik bir örnekle desteklenmiştir

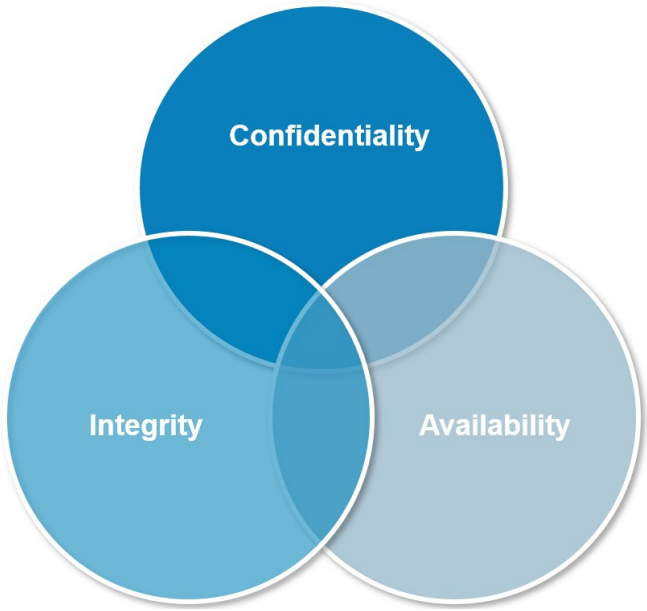
Öğrenme Materyalinin İçeriği

1. **Bilgi güvenliği**

Bilgi güvenliği, bilgilere yetkisiz veya yetkisiz erişim, kullanım, değişiklik, ifşa, imha, değiştirme ve zarar verilmesini önlemektir. Gizlilik, Bütünlük ve Erişilebilirlik adı verilen üç temel unsurdan oluşur (Şekil 1). Bu üç temel güvenlik öğesinden herhangi biri zarar görmüşse, bir güvenlik açığı oluşur.

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



Şekil 1. Bilgi güvenliği unsurları

- Gizlilik: Bilgilerin yetkisiz erişime ve yetkisiz erişime karşı korunmasıdır.
- Bütünlük: Bilgiler yetkisiz kişiler tarafından değiştirilmez.
- Erişilebilirlik: Bilgi, yetkili kişiler tarafından ihtiyaç duyulduğunda erişilebilir ve kullanılabilir.

1.1. Bilgi güvenliği politikası nedir?

Güvenlik tehditleri sürekli olarak gelişmektedir ve uyumluluk gereksinimleri giderek daha karmaşık hale gelmektedir. Kuruluşlar, her iki zorluğu da kapsayacak kapsamlı bir bilgi güvenliği politikası oluşturmalıdır. Bilgi güvenliği ilkesi (ISS), bir kuruluştaki tüm son kullanıcıların ve ağların minimum BT güvenliği ve veri koruma güvenliği gereksinimlerini karşılamasını sağlamak için tasarlanmış bir dizi kural, politika ve prosedürdür. Bir bilgi güvenliği politikası, bir güvenlik programını koordine etmeyi ve uygulamayı ve güvenlik önlemlerini üçüncü taraflara ve dış denetçilere iletmeyi mümkün kılar.

1.2. Bilgi Güvenliği Politikasının Amacı Nedir?

Bir bilgi güvenliği politikası, korumaları yürürlüğe koymayı ve verilerin dağıtımını yalnızca yetkili erişime sahip olanlarla sınırlamayı amaçlamaktadır. Kuruluşlar aşağıdakileri yapmak için ISS'ler oluşturur:

- Bilgi güvenliğine genel bir yaklaşım oluşturmak

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.

- Belge güvenliği önlemleri ve kullanıcı erişim denetimi politikaları
- Verilerin, ağların, mobil cihazların, bilgisayarların ve uygulamaların kötüye kullanımı gibi güvenliği ihlal edilmiş bilgi varlıklarının etkisini tespit edin ve en aza indirin
- Kuruluşun itibarını korumak
- ENISA, NIST, GDPR, HIPAA ve FERPA gibi yasal ve düzenleyici gerekliliklere uymak
- Kredi kartı numaraları gibi müşterilerinin verilerini koruma
- Kimlik avı, kötü amaçlı yazılım ve fidye yazılımı gibi gerçek veya algılanan siber güvenlik riskleriyle ilgili şikayetlere ve sorgulara yanıt vermek için etkili mekanizmalar sağlayın
- Önemli bilgi teknolojisi varlıklarına erişimi, kabul edilebilir bir kullanıma sahip olanlarla sınırlandırın

1.3. Bilgi Güvenliği Politikası Neden Önemlidir?

Tüm uyumluluk gereksinimlerini karşılayan etkili bir bilgi güvenliği politikası oluşturmak, veri sızıntıları ve veri ihlalleri gibi güvenlik olaylarını önlemede kritik bir adımdır.

ISS'ler yeni ve yerleşik kuruluşlar için önemlidir. Dijitalleşmenin artması, her çalışanın veri ürettiği ve bu verilerin bir kısmının yetkisiz erişime karşı korunması gerektiği anlamına gelir. Sektörünüze bağlı olarak, yasalar ve yönetmeliklerle bile korunabilir.

Hassas veriler, kişisel olarak tanımlanabilir bilgiler (PII) ve fikri mülkiyet, diğer verilerden daha yüksek bir standartta korunmalıdır. İster beğenin ister beğenmeyin, bilgi güvenliği (InfoSec) kuruluşunuzun her düzeyinde önemlidir.

Bilgi güvenliği ilkeleri bir kuruluş için aşağıdaki avantajlara sahip olabilir:

- **Veri bütünlüğünü, kullanılabilirliğini ve gizliliğini kolaylaştırır-** Etkili bilgi güvenliği politikaları, veri bütünlüğünü, kullanılabilirliğini ve gizliliğini tehdit eden vektörlere karşı koruma sağlayan kuralları ve süreçleri standartlaştırır.
- **Hassas verileri korur — I**nformation güvenlik politikaları, fikri mülkiyetin ve kişisel olarak tanımlanabilir bilgiler (PII) gibi hassas verilerin korunmasına öncelik verir.
- **Güvenlik olayları riskini en aza indirir —** Bir bilgi güvenliği ilkesi, kuruluşların güvenlik açıklarını ve riskleri tanımlamak ve azaltmak için prosedürler tanımlamasına yardımcı olur. Ayrıca, bir güvenlik olayı sırasında hasarı en aza indirmek için hızlı yanıtları da ayrıntılarıyla açıklar.
- **Kuruluş genelinde güvenlik programları yürütür -**Güvenlik politikalarını, prosedürleri operasyonel hale getirmek için çerçeve sağlar.

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.

- **Üçüncü taraflara açık bir güvenlik beyanı sağlar** — Bilgi güvenliği ilkeleri, kuruluşun güvenlik duruşunu özetler ve kuruluşun BT kaynaklarını ve varlıklarını nasıl koruduğunu açıklar. Müşterilerin, iş ortaklarının ve denetçilerin üçüncü taraf bilgi taleplerine hızlı yanıt verilmesini kolaylaştırır.
- **Mevzuat gereksinimlerine uyulmasına yardımcı olur** — Bir bilgi güvenliği politikası oluşturmak, kuruluşların yasal gereksinimlerle ilgili güvenlik açıklarını belirlemesine ve bunları ele almasına yardımcı olabilir.

1.4. Bilgi Güvenliği Politikasında Neler Olmalıdır?

Bir bilgi güvenliği politikasının sıfırdan oluşturulması zor olabilir; sağlam olması ve kuruluşunuzu tüm uçlardan koruması gerekir. Tüm yazılım, donanım, fiziksel parametreler, insan kaynakları, bilgi ve erişim kontrolünü kapsamalıdır. Ayrıca esnek olması ve revizyon ve güncelleme için alana sahip olması ve en önemlisi pratik ve uygulanabilir olması gerekir. Bir bilgi güvenliği politikası geliştirirken hüsnükuruntulu düşünme size yardımcı olmaz. Şirketiniz ve politikayı yürütmekten sorumlu olacak çalışanlar için işe yarayan bir politika geliştirmek için ana paydaşlarla birlikte çalışmanız gerekir.

1. Kabul Edilebilir Kullanım Politikası

Bu politika, kuruluşunuzda bilgisayar ekipmanının ve internetin kabul edilebilir kullanımını özetler. İnternetin veya bilgisayarların yanlış kullanımı, şirketinizi virüs saldırıları, güvenliği ihlal edilmiş ağ sistemleri, hizmetler ve yasal sorunlar gibi risklere karşı açar, bu nedenle kabul edilebilir kullanımın ne olduğunu ve neyin olmadığını yazılı olarak bulundurmak önemlidir.

Kabul edilebilir bir kullanım politikası, çalışanların masalarından uzaktayken bilgisayarlarını kilitlemek veya hassas bilgiler içerebilecek tabletleri veya diğer elektronik cihazları korumak gibi şirketin ekipmanlarını koruma konusunda nelerden sorumlu olduklarını ana hatlarıyla belirtmelidir. Ayrıca, şirketin haklarının ne olduğunu ve şirketin ekipman ve ağında hangi faaliyetlerin yasaklanmadığını da belirtmelidir.

2. Temiz Masa Politikası

Temiz masa politikası, fiziksel varlıkların ve bilgilerin korunmasına odaklanır. İdeal olarak, bu politika tüm hassas ve gizli materyallerin kullanılmadığında veya bir çalışanın masasından ayrılmasıyla kilitlenmesini veya başka bir şekilde güvence altına alınmasını sağlayacaktır. Bu ilke, çalışanlar, fikri mülkiyet, müşteriler ve satıcılar hakkındaki hassas bilgilerin depolanabileceği ve bunlara erişilebileceği yerler gibi temiz bir masa tutmak için minimum gereksinimleri belirlemelidir. Ayrıca, ne tür malzemelerin parçalanması veya atılması gerektiği, bir yazıcıdan belge almak için parolaların kullanılması gerekip gerekmediği ve fiziksel bir kilitle hangi bilgilerin veya mülklerin güvence altına alınması gerektiği gibi şeyleri de kapsamalıdır. Herhangi bir bilgi güvenliği politikasının ortak ve önemli bir parçası olmasının yanı sıra, temiz masa politikası ISO

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

27001/17799 uyumludur ve işletmenizin bir sertifika denetimini geçmesine yardımcı olacaktır.

3. *Veri İhlali Müdahale Politikası*

Bu, olay müdahale planı olarak da bilinir. Veri ihlali yanıt politikasının amacı, kuruluşunuzun bir veri ihlaline nasıl yanıt vereceğine ilişkin hedefleri ve vizyonu oluşturmaktır. Bu plan, kuruluşunuzun olay müdahale süreci boyunca veri varlıklarını nasıl korumayı planladığını ayrıntılarıyla açıklayacağından, siber saldırı kurbanı olma risklerini azaltmaya yardımcı olacaktır.

Bu politika, ihlalin tanımı, personel rolleri ve sorumlulukları, standartlar ve metrikler, raporlama, düzeltme ve geri bildirim mekanizmaları dahil olmak üzere kimler için geçerli olduğunu ve ne zaman yürürlüğe gireceğini tanımlamalıdır.

4. *Olağanüstü Durum Kurtarma Planı İlkesi*

Bu politika, bir veri ihlali müdahale planından farklıdır, çünkü bir felaket durumunda veya uzun süreli hizmet gecikmesine neden olan herhangi bir olayda ne yapılması gerektiğine ilişkin genel bir acil durum planıdır. Bu ilke, büyük bir kesintiye neden olan herhangi bir olağanüstü durum sırasında veya sonrasında sistemleri, uygulamaları ve verileri kurtarma işlemini açıklamalıdır. Bu olağanüstü durum kurtarma planı yıllık olarak güncellenmelidir.

Acil durum planı şu unsurları kapsamalıdır:

- Acil durum sosyal yardım planı. Kimlerle iletişime geçilmesi gerektiğini, ne zaman iletişim kurulması gerektiğini ve onlarla nasıl iletişime geçeceğinizi açıkça listeleyin.
- Veraset planı. Normal personelin görevlerini yerine getiremediği durumlarda sorumluluk akışını tanımlayın.
- Veri sınıflandırma planı. Tüm sistemlerde depolanan tüm verileri, kritikliğini ve gizliliğini ayrıntılandırın.
- Hizmet listesinin kritikliği. Sağlanan tüm hizmetleri ve önem sıralarını listeleyin.
- Veri yedekleme ve geri yükleme planı. Hangi verilerin nerede ve ne sıklıkta yedeklendiğini ayrıntılandırın. Ayrıca verilerin nasıl kurtarılabileceğini de açıklayın.
- Ekipman değiştirme planı. Müşterilere hizmet sağlamaya devam etmek için hangi altyapı hizmetlerinin gerekli olduğunu açıklayın.
- Kamu iletişimi. Dış PR işlevine kimin sahip olacağını belgeleyin ve hangi bilgilerin paylaşılabileceği ve paylaşılması gerektiği konusunda yönergeler sağlayın.
- Yönetim ekibinin olağanüstü durum kurtarma planını test etmek için zaman ayırması önemlidir. Masa üstü egzersizleri olarak da bilinen bu testler sırasında amaç, planlama aşamasında planın başarısız olmasına neden olabilecek açık olmayabilecek sorunları belirlemektir. Bu şekilde, ekip bir felaket gerçekleşmeden önce planı ayarlayabilir.

5. *E-posta Politikası*

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.

E-posta, her türden işletme için kritik bir iletişim kanalıdır ve e-postanın kötüye kullanılması, gizli bilgileri dağıtmak için e-posta kullanan çalışanlar veya ağınızı yanlışlıkla bir virüse maruz bırakan çalışanlar olsun, şirketinizin güvenliği için birçok tehdit oluşturabilir. Şirketiniz adına çalışan tüm çalışanların, yüklenicilerin ve aracıların uygun e-posta kullanımını anlaması ve gerektiğinde e-postaları arşivlemek, işaretlemek ve incelemek için politika ve prosedürlerin oluşturulması önemlidir.

Bu politikanın, şirket e-posta adreslerinin uygun kullanımını ana hatlarıyla belirtmesi ve ne tür iletişimlerin yasak olduğu, ekler için veri güvenliği standartları, e-posta saklama ile ilgili kurallar ve şirketin e-postaları izleyip izlemediği gibi konuları kapsaması gerekir. Bu politika aynı zamanda çalışanlarınız için açıkça düzenlenmelidir, böylece e-posta adreslerini kullanma sorumluluklarını ve şirketin e-postaların doğru şekilde kullanılmasını sağlama sorumluluğunu anlarlar. Bu e-posta politikası, çalışanların e-postalarını kötüye kullanmasını yakalamak için bir "gotcha" politikası oluşturmakla ilgili değil, çalışanların neyin neye izin verilip neyin verilmediğini anlamadıkları için bir e-postayı kötüye kullandıkları bir durumdan kaçınmakla ilgilidir.

6. Son Kullanıcı Şifreleme Anahtarı Koruma İlkesi

Şirketinizdeki veya son kullanıcılarınıza dağıtılan belirli belge ve iletişimlerin güvenlik amacıyla şifrelenmesi gerekebilir. Bu şifreleme anahtarlarının açıklanmaması veya hileli bir şekilde kullanılmaması için bu şifreleme anahtarlarını korumak için bir ilke uygulayın.

Bu politika, şifreleme anahtarlarını korumaya yönelik tüm gereksinimleri ana hatlarıyla belirtmeli ve bunları güvende tutmak için belirli operasyonel ve teknik denetimleri listelemelidir. Bu, kurcalamaya karşı dayanıklı donanım, yedekleme yordamları ve bir şifreleme anahtarının kaybolması, çalınması veya hileli bir şekilde kullanılması durumunda ne yapılması gerektiği gibi şeyleri içerir.

7. Parola Koruma Politikası

Çalışanlarınızın büyük olasılıkla günlük olarak takip etmeleri ve kullanmaları gereken sayısız parolaları vardır ve işletmenizin bilgisayarları, e-posta hesapları, elektronik cihazları ve verilerinize veya ağınıza sahip oldukları herhangi bir erişim noktası için güçlü parolalar oluşturmak için açık ve net standartları olmalıdır.

Bu politikanın ayrıca çalışanların parolalarıyla neler yapabileceğini ve yapamayacağını da ana hatlarıyla belirtmesi gerekir. Şifrelerini bir e-postaya koymamaları veya meslektaşlarıyla paylaşmamaları gerektiği açık görünebilir, ancak bunun herkes için ortak bir bilgi olduğunu varsaymamalısınız. Çalışanlarınıza güçlü parolalar oluşturmak için ihtiyaç duydukları tüm bilgileri verin ve veri ihlali riskini en aza indirmek için onları güvende tutun.

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

Son olarak, bu politika, şirketiniz tarafından işletilen tüm uygulamaların veya web sitelerinin kullanıcı parolalarını güvende tutmak için güvenlik önlemlerine uyduğundan emin olmak için geliştiricilerinizin ve BT personelinizin ne yapması gerektiğini özetlemelidir.

Son on yılda dünya genelinde yapılan araştırmalar, kullanıcıların en çok tercih ettiği şifrelerin ise şu şekilde olduğunu göstermektedir:

- 123456
- password
- Qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Yıllık uyarılara rağmen, bu liste çok fazla değişmedi. Bunun için kullanıcıların bir dizi şifre belirleme kuralına uymaları önerilir. Bu kurallar aşağıda listelenmiştir:

- Minimum karakter gereksinimini karşılamak gibi karmaşıklık gereksinimlerini ayarlama
- Daha önce kullanılan şifreleri seçmemek
- Parolaları periyodik olarak ve belki de sık sık değiştirme
- Kullanılan şifreler, yukarıdaki listede olduğu gibi yaygın ve zayıf kullanılan şifrelerden seçilmemelidir.

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), şifreleri belirlemek ve belirli standartlara ulaşmak için şifre politikaları sorununu çözmeyi amaçlamıştır. NIST, parolalar ve bunların nasıl yönetilmesi ve depolanması gerektiği ile ilgili ayrıntıları belirler. Buna göre, olası şifreler yaygın olarak kullanılan ve bilinen değerlerin bir listesine göre kontrol edilmelidir. Parolaları belirlerken dikkat edilmesi gereken noktalar şunlardır:

- Kullanıcı tarafından sağlanan parolalar en az sekiz alfasayısal karakterden oluşmalıdır.
- Bunlar, önceki ihlallerden elde edilen şifreler olmamalıdır.
- Sözlük kelimeleri olmamalıdır.
- Doğum tarihleri gibi 1900-2020 yılları arasında tarih olmamalıdır.
- Yinelenen veya sıralı karakterler yok (ör. aaaaaaaa veya 1234abcd)
- Hizmetin adı, kullanıcı adı ve türevleri gibi kullanım amacına özgü kelimeler olmamalıdır.

Şifreler belirlenirken yukarıdaki kriterler dikkate alınmalı ve karmaşık yapılara sahip şifreler oluşturulmalıdır.

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

Parola karmaşıklığı : Parola karmaşıklığı, bir parola için güçlü olan parola sayısı olarak tanımlanır ve bir dizi kuralı karşıladığını kastediyoruz. Parola karmaşıklığının anahtarı Kurallar aşağıdaki gibidir:

- Parola, hesap adını veya hesap adının varyasyonlarını içeremez.
- Parola hem büyük harf (A-Z) hem de küçük harf (a-z) içermelidir.
- Özel karakterler (**~! @ # $% ^ & * _- + = '| \ () {} [] :;" '<>,.? /)** (Bunlar genellikle ALT tuşuyla birlikte görünen karakterlerdir. Ancak, Euro sembolleri gibi para birimleri özel karakterler olarak sayılmaz).
- Minimum karakter sayısına uyulmalıdır. Bu değer sistemden sisteme, kullanıcıdan kullanıcıya değişir.

Minimum parola uzunluğu 8 karakter, önerilen karakter ise 12 karakter olmalıdır.
Yukarıda listelenen kurallara göre en az 8 karakterden oluşan şifreler oluşturulduğunda, tek bir şifre için en az 218.340.105.584.896 farklı olasılık anlamına gelir. Oluşturulan şifrenin olasılığı, kaba kuvvet saldırısını çok zorlaştırır, ancak şifrenin kırılması hala imkansız değildir. Kırılması imkansıza yakın bir şifre için, şifre karakterlerinin sayısını artırmak gerekir. Minimum karakter sayısı ne kadar yüksek olursa, şifreyi kırmak o kadar uzun sürer.
Parola karmaşıklığının faydalarına ek olarak, bazı zorlukları da beraberinde getirir. Bunlardan en önemlilerinden biri şifreyi unutmak. Daha uzun ve özel karakterler içeren bir parolayı hatırlamak zordur. Özellikle tüm şifreler farklı olduğunda, hatırlamak ve başkalarıyla karıştırmamak zordur. Bu nedenle şifre oluşturulurken belli bir mantık izlenmelidir.

Örneğin;

- 3 çocuklu bir ailenin 2. çocuğuyum!

Kendi gerçek hayatınıza dayanarak böyle bir cümle yazabilirsiniz. Cümlenin ilk karakterlerini ve özel karakterlerini aldığınızda, **3cba2.c!** gibi bir şifre elde edersiniz!

- 19 Temmuz'da Bu Web Sitesine (eğitim hakkında) Üye Oldum.

"19 Temmuzda bu web sitesine (eğitim hakkında) üye oldum" gibi bir cümleyi, web sitesinin ilgi alanına ve üyelik tarihine göre özelleştirebilir, böylece unutmayabilirsiniz. İlk karakterlerini ve özel karakterlerini aldığınızda
19TBWS(eh)UO. gibi bir şifre alacaksınız.

8. Güvenlik Yanıt Planı İlkesi

Bir güvenlik yanıt planı, veri ihlali gibi bir tür güvenlik olayı durumunda her ekibin veya iş biriminin ne yapması gerektiğini ortaya koyar. SANS Enstitüsü'ne göre, "bir ürün açıklaması, iletişim bilgileri, yükseltme yolları, beklenen hizmet düzeyi sözleşmeleri (SLA), önem derecesi ve etki sınıflandırması ve azaltma / düzeltme zaman çizelgeleri" tanımlamalıdır.

Bir güvenlik müdahale planı politikasının anahtarı, tüm farklı ekiplerin çabalarını entegre

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.

etmelerine yardımcı olmasıdır, böylece meydana gelen güvenlik olayı ne olursa olsun mümkün olan en kısa sürede azaltılabilir. Her departmanın kendi yanıt planları olsa da, güvenlik yanıt planı ilkesi, bir güvenlik olayına verilen yanıtın hızlı ve kapsamlı olduğundan emin olmak için birbirleriyle nasıl koordine edeceklerini ayrıntılarıyla açıklar.

1.5. Bilgi Güvenliği Politikası Örnekleri

Başarılı bir siber güvenlik planı oluşturmak için 5 ana konunun göz önünde bulundurulması gerekmektedir.

a. ***Tanımlama: Kuruluş,*** çabalarına öncelik verebilmesi için karşılaştığı siber güvenlik risklerini anlamalıdır.

b. ***Koruma***: Bu, veri varlıklarını korumak ve potansiyel bir siber güvenlik olayının etkisini sınırlamak veya içermek için uygun önlemleri almakla ilgilidir. Bu, kuruluş içindeki personel üyelerini risklerin farkında olmaları için eğitmeyi ve güçlendirmeyi, ağ güvenliğini ve varlıklarını korumaya odaklanan prosedürler oluşturmayı ve bir siber suçlunun mevcut korumaları atlayabilmesi durumunda bir şirketi finansal olarak korumak için potansiyel olarak siber sorumluluk sigortasını kullanmayı içerir.

c. ***Algıla***: Bir siber saldırının oluşumunu keşfetmeye yardımcı olan faaliyetleri ana hatlarıyla belirtin ve olaya zamanında yanıt verilmesini sağlayın. Bir siber saldırıyı hızlı ve verimli bir şekilde teşhis etmek için şirketler, verilerin tehlikeye girdiği göründüğünde onları uyaran veri sınıflandırma, varlık yönetimi ve risk yönetimi protokollerini uygulamalıdır.

d. ***Yanıtla***: Siber güvenlik tehditlerinin tespitini takiben yapılması gereken uygun eylemleri belgeleyin. Bir şirketin yanıtı, personel, hissedarlar, ortaklar ve müşterilerin yanı sıra gerektiğinde kolluk kuvvetleri ve hukuk müşaviri ile doğru ve kapsamlı bir iletişim içermelidir.

e. ***Kurtarma***: Bir kuruluşun siber saldırı nedeniyle bozulan tüm yetenekleri veya hizmetleri nasıl kurtarabileceğini ve geri yükleyebileceğini belirleyin.

Hemen hemen her güvenlik standardı, bir tür olay müdahale planı için bir gereklilik içermelidir, çünkü en sağlam bilgi güvenliği planları ve uyumluluk programları bile veri ihlaline maruz kalabilir.

1.6. Bilgi Güvenliği Politikası 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.

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

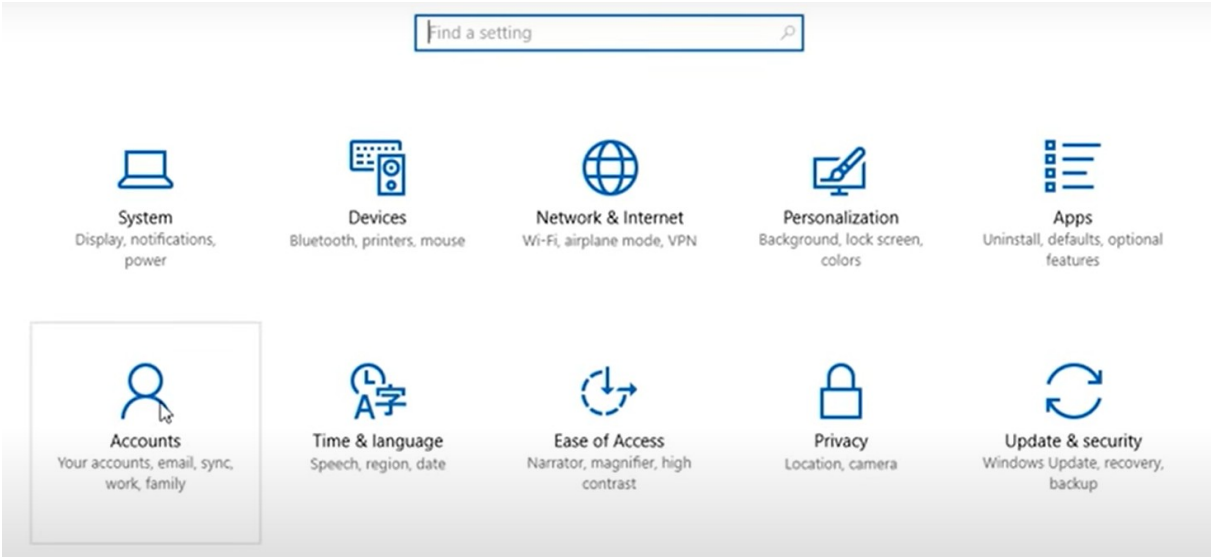
1. Oturumunuzu kilitleyin: Biyometri (bir kişinin ölçülebilir biyolojik izleri), güvenlik anahtarları veya mobil cihazınızdaki bir uygulama aracı tarafından oluşturulan benzersiz bir tek seferlik kod gibi mevcut en güçlü kimlik doğrulama araçlarını etkinleştirerek çevrimiçi hesaplarınızı güçlendirin. Kullanıcı adlarınız ve şifreleriniz e-posta, bankacılık ve sosyal medya gibi hesapları korumak için yeterli olmayabilir.

Alıştırmalar-1:

Bilgisayardan kalktığınızda bilgisayarın otomatik olarak kilitlenmesini sağlamak için.

Adım-1: Windows Ayarları düğmesine tıklayın.

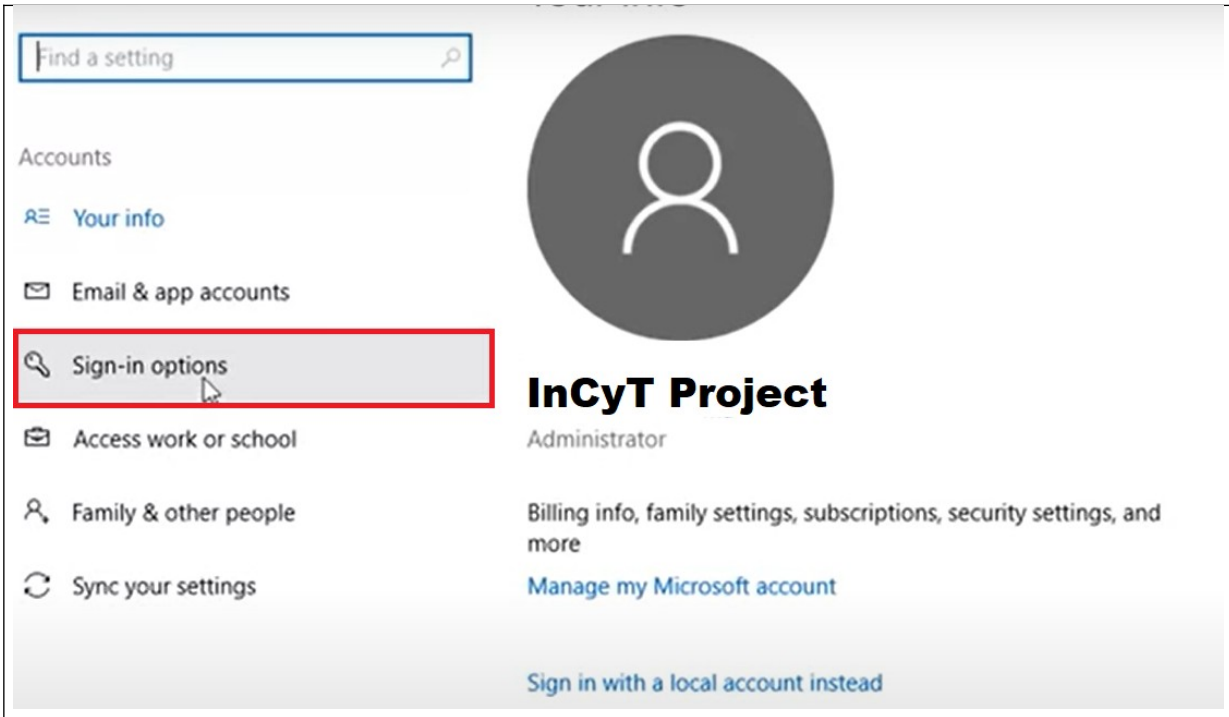
Adım-2: Hesaplar sekmesini tıklayın.



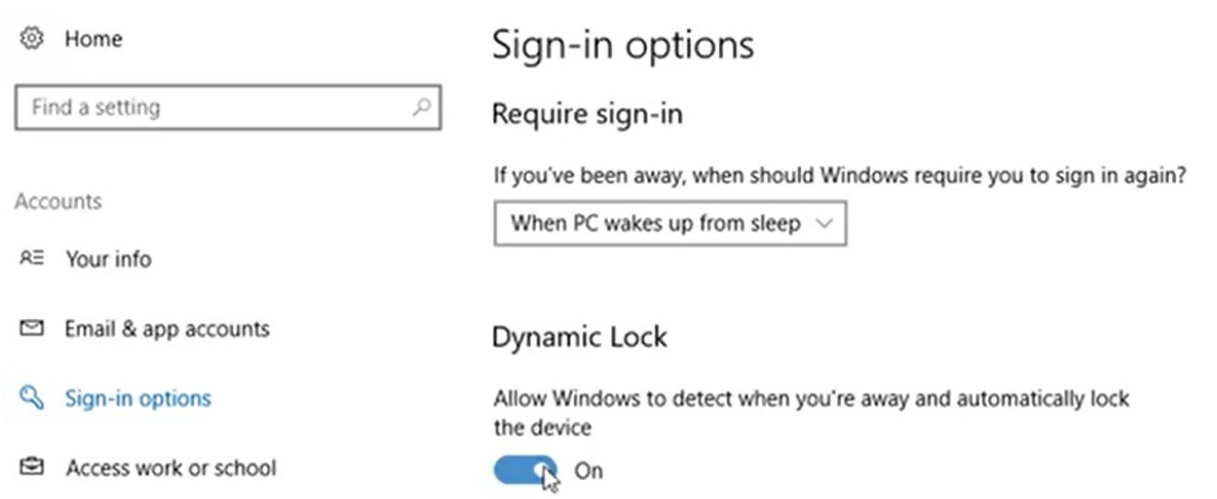
Adım-3: Oturum açma bölümüne tıklayın.

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



Adım-4: Dinamik Kilit özelliğinde etkinleştirin.



2- Güçlü bir şifre oluşturun: Şifrenin bilgi güvenliğinde önemli bir yeri vardır. Zayıf şifreler şifre kırma programları ile kısa sürede çözülebilir. Bu nedenle tüm cihaz ve hesaplarda şifre oluştururken ve kullanırken aşağıdaki kuralları göz önünde bulundurarak azami özen göstermek gerekir. Şifre genellikle bilgisayar sistemlerinde birçok yerde kullanılır. Bir e-posta hesabı oluştururken, bilgisayar oturum açarken bir parola ayarlarken ve dosyalara erişimi yasaklarken bir parola kullanırız. Ancak, parolalar zayıf veya tahmin edilebilir olmamalıdır. Şifreler aşağıdaki kriterlere göre oluşturulmalıdır:

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

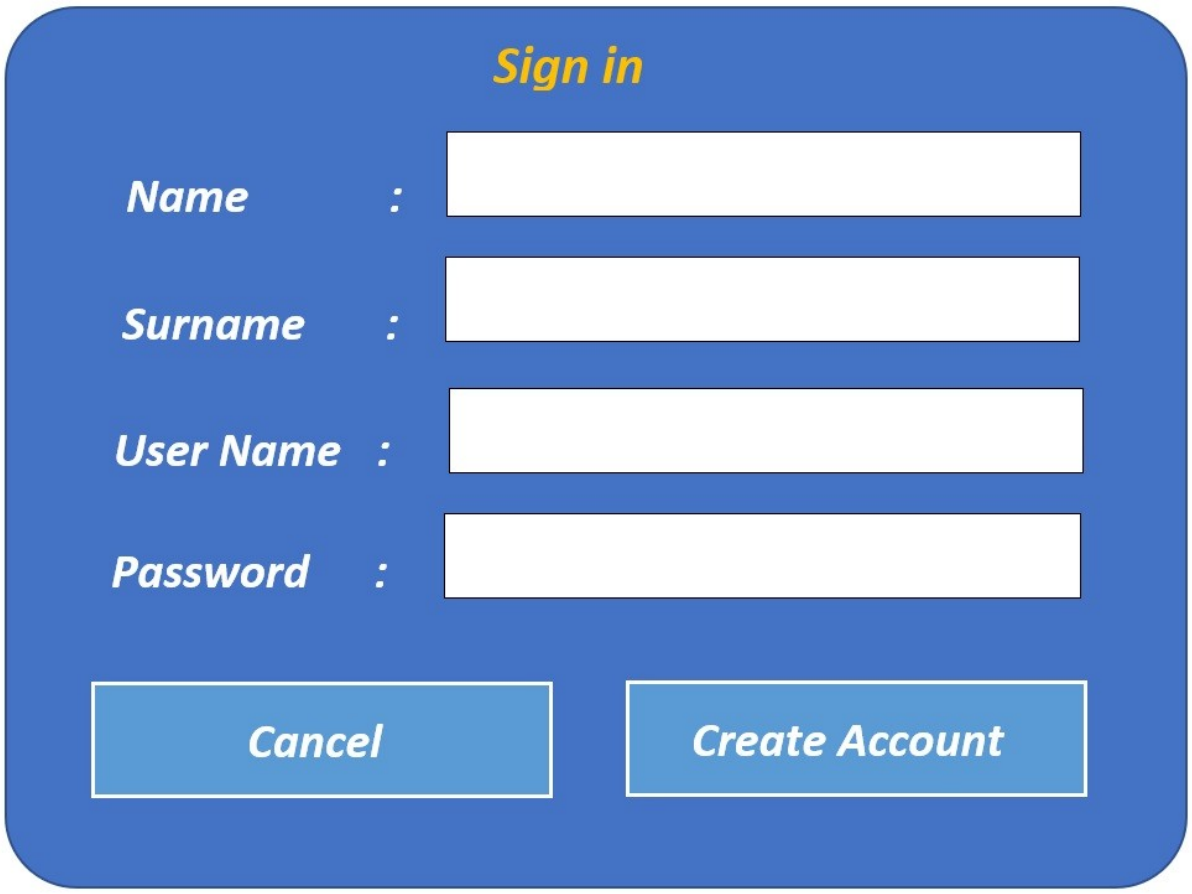
a. Parolalar en az 8 karakter uzunluğunda olmalı ve ***en az*** bir büyük harf, bir küçük harf, bir sayı ve bir özel karakter (.-+=_,!@$#*%<>[]{}) içermelidir.
b. Parola alanı boş veya varsayılan olarak bırakılmamalıdır; ***123456, 01062022, qwerty, şifre vb.*** herhangi bir sözlükte bulunabilecek kelimeler gibi öngörülebilir ve kolayca kırılabilecek şekilde belirlenmemelidir.
c. Parolalar **kişisel bilgiler** (çocuğunuzun adı, doğum tarihi veya kurum adı) içermemelidir.
d. ***Farklı*** sistemler ve hesaplar için farklı şifreler oluşturulmalıdır.
e. Şifreler sık sık değiştirilmelidir (en az 6 ayda bir).
f. Parolalar başkaları tarafından fark edilebilecek yerlere yazılmamalıdır (kâğıda yazılarak bilgisayarın yanında bırakılması gibi) ve bir bilgisayarda veya herhangi bir dijital ortamda şifrelenmeden açık metin olarak saklanmamalıdır.
g. Hiçbir personel veya öğrenci şifresini (e-posta şifresi, e-imza şifresi, PC şifresi vb.) başka bir kişiyle ***paylaşmamalıdır***. Kullanıcılar, paylaşım durumunda doğabilecek tüm yasal sorumluluğun kendisine ait olacağını bilmelidir.
h. Benzersiz hesap, benzersiz parola: Her hesap için ayrı bir parolaya sahip olmak, siber suçluların engellenmesine yardımcı olur. En azından, iş ve kişisel hesaplarınızı ayırın ve kritik hesaplarınızın en güçlü şifrelere sahip olduğundan emin olun.
i. Unutmayın ve güvende tutun: Güçlü parolalar oluşturmak ve hatırlamak zordur. Parolalarınızı yalnızca sizin için anlamlı ve akılda kalıcı olacak şekilde ayarlayın veya güvenli bir yerde ve biçimde saklayın. Alternatif olarak, parolalarınızı takip etmek için parola yöneticisi gibi bir hizmet kullanabilirsiniz.

Alıştırmalar-2:

Kurumsal e-posta servis sağlayıcınız veya genel bir e-posta servis sağlayıcısının uygulaması ya da web sitesi aracılığıyla bir e-posta hesabı oluştururken parola güvenliği

Adım-1: Web sitesini veya uygulamayı açın.
Adım-2: Bir hesap oluşturmak için kişisel bilgilerinizi girin.

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.



Adım-3: Bir şifre oluştururken, büyük harf, küçük harf, rakam, sembol kombinasyonlarını birlikte kullanın.
Şifrenin kullanıcı tarafından hatırlanmasını kolaylaştırmak için bazı kodlamalar yapılabilir. Örneğin konuya uygun bir cümle yazabilir ve yazdığınız cümlenin ilk karakterlerini, sayılarını ve özel karakterlerini kullanabilirsiniz.

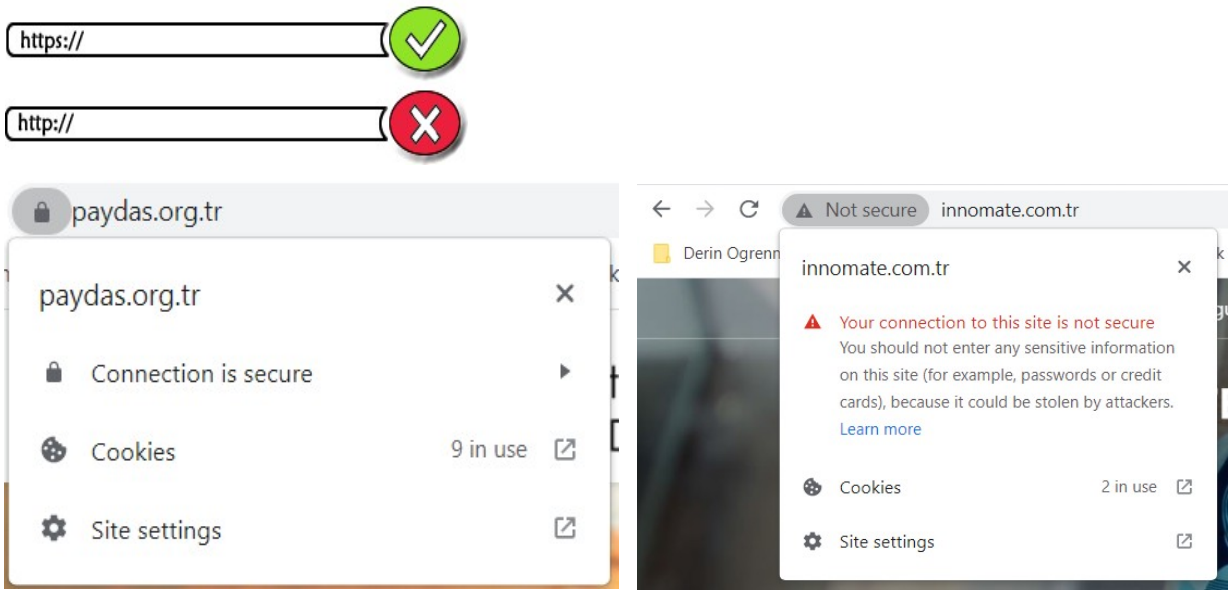
This **c**ybersecurity **p**roject **i** s s upported **b**y **E**rasmus**+ 2021**

Adım-4: Şifremizi belirledik; **TcpisbE+2021**
Adım-5: Şifrenin en az 8 karakterden oluştuğundan emin olun. 12 karakter tercih edilir. Kullandığımız şifrenin 12 karakterden oluştuğu için uygun olduğu söylenebilir.

3- Güvenli sitelere erişim (Güvenli Tarayıcı): Alışveriş yapmak veya haber okumak için çevrimiçi olduğunuzda bir tarayıcı kullanıyorsunuz demektir. Tarayıcılar, İnternet ile etkileşim kurmanın başlıca yollarından biridir. Sonuç olarak, tarayıcılar siber saldırganlar için birincil hedeflerdir. Her zaman tarayıcınızın en son sürümünü kullanın ve güvenlik kalkanınızı tarayıcı saldırılarına karşı güçlü tutun. Güncellenmiş tarayıcılar en son güvenlik yamalarına sahiptir ve siber saldırganların

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.

yararlanması çok daha zordur. En son tarayıcı güncellemesine sahip olup olmadığınızdan emin değil misiniz? Doğrulamak için Teknik Destek Ekibine veya Bilgi Güvenliği Ekibine başvurun. Tarayıcınızdan bir uyarı aldığınızda web sitelerine bağlanmayarak çevrimiçi ortamda güvende kalın. Modern tarayıcılar, zarar vermek üzere tasarlanmış belirli kötü amaçlı web sitelerini tanıyabilir. Tarayıcınız ziyaret etmek üzere olduğunuz web sitesinin tehlikeli olduğunu size bildirirse, o web sayfasını kapatın ve aradığınız bilgileri daha güvenli bir web sitesinde bulmaya çalışın. Hassas bilgileri çevrimiçi göndermeden önce, örneğin kredi kartı bilgilerinizi çevrimiçi alışveriş için gönderirken, tarayıcınızın bir şifreleme işareti olan HTTPS kullandığından emin olun. Şifreleme, bilgisayarınız ile hedef arasında iletilen bilgileri karıştırır, böylece yalnızca yetkili web sitesi okuyabilir. Güvenli bir bağlantı için, HTTPS ile başlayan web sitesi adresi ve durum çubuğunda bir asma kilit simgesi gibi şifreleme işaretlerini arayın.



Şekil 2. Güvenli ve Güvenli Değilweb siteleri

Eklentiler; oyun oynamak, film izlemek veya metin düzenlemek gibi ek özellikler için kullanılan tarayıcılara eklenen küçük yazılım parçalarıdır. Tarayıcınıza yüklenen her eklenti potansiyel olarak ek güvenlik açıkları ekler. Bunlara kesinlikle ihtiyacınız varsa ve yalnızca önceden onay aldıysanız, eklentileri tarayıcınıza yükleyin. Yüklendikten sonra, tarayıcınızda olduğu gibi her zaman eklentinin en son sürümünü kullanın. Son olarak, bir web sitesini ziyaret etmeyi bitirdikten sonra, oturumunuzun kapalı olduğundan emin olun. Bu, tarayıcıyı kapatmadan önce hassas oturum açma bilgilerini ve parola bilgilerini kaldırır. Güvenli tarama davranışınızın ve güvenlik kalkanınızın güçlendirildiğini unutmayın.

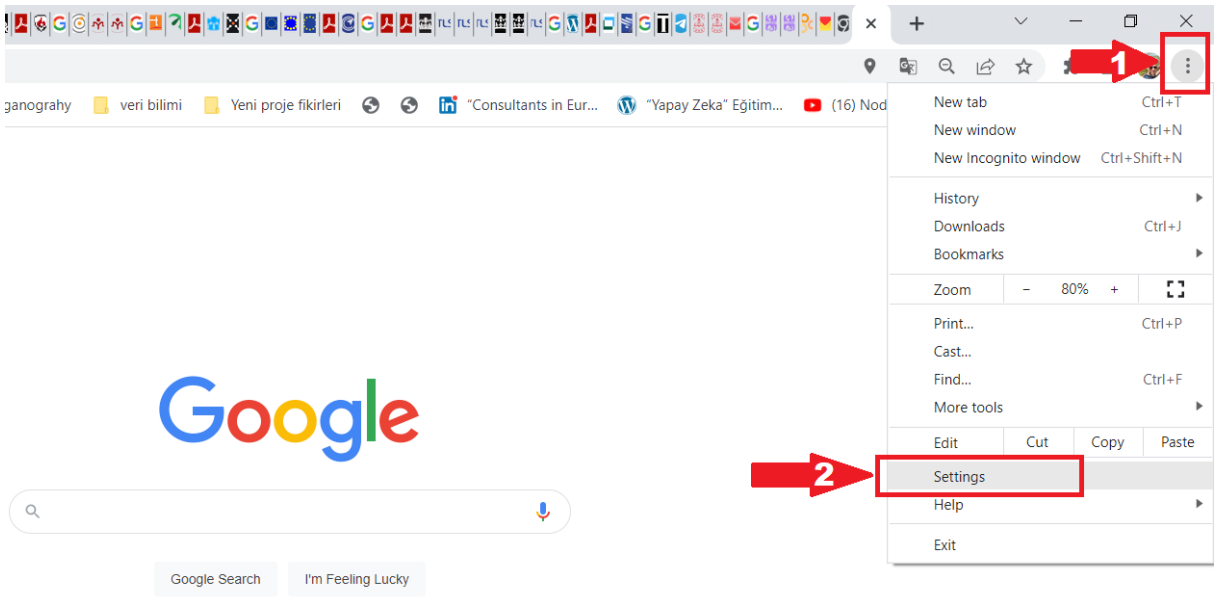
Alıştırmalar-3:

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.

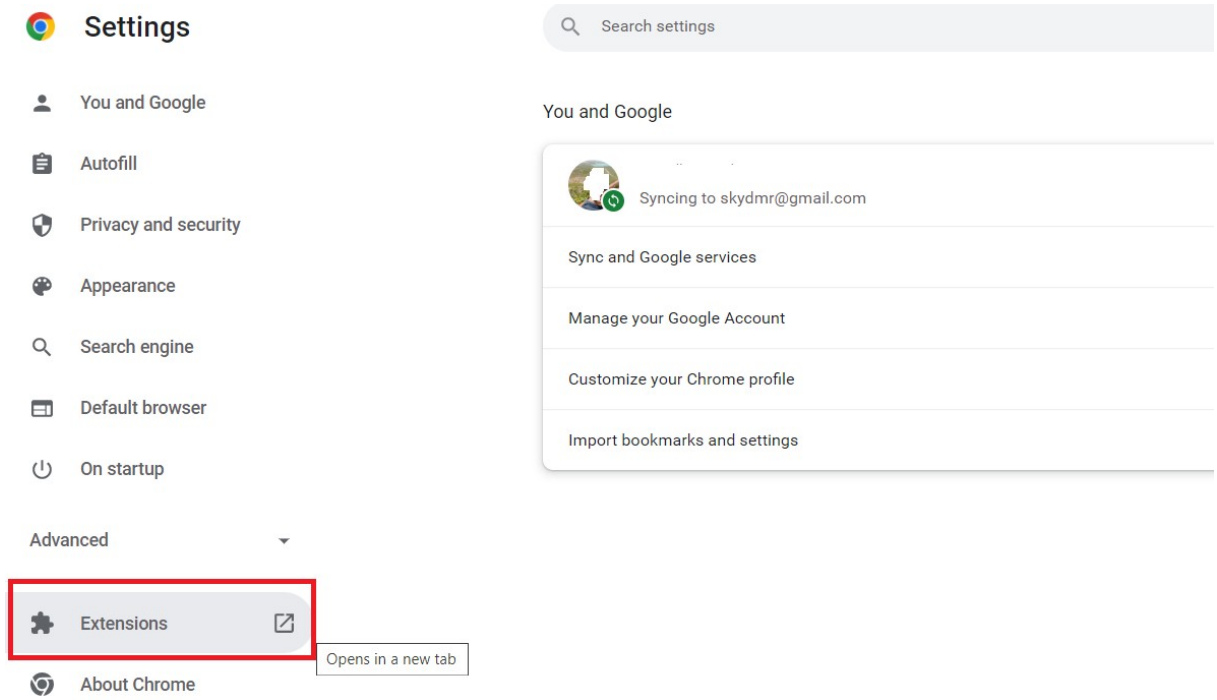
Co-funded by the Erasmus+ Programme of the European Union

Eklentileri web tarayıcısında düzenlemek için aşağıdaki adımları izleyin.

Adım-1: Web tarayıcınızı açın ve "Kostüm ve Kontrol..." düğmesini sol üst köşedeki düğme (1). Açılır menüden "Ayarlar" sekmesine tıklayın (2).



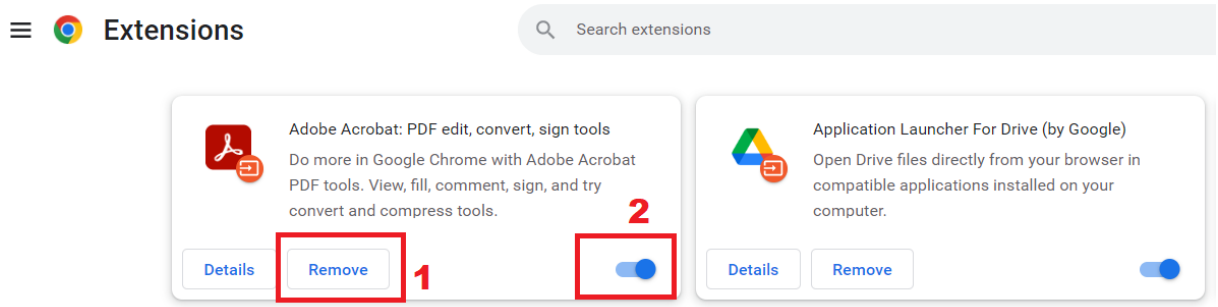
Adım-2: Açılan pencerede "Uzantılar" düğmesini tıklayın.



Adım-3: Tarayıcınızda yüklü olan eklentileri bu ekranda görebilirsiniz. Eklentiyi silmek istiyorsanız, "Romove" düğmesine basarak silebilirsiniz (1). Eklentinin etkin olmamasını

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.

istiyorsanız, "Açma-Kapama" düğmesinden (2) devre dışı bırakabilirsiniz.



4. E-posta, Mesajlaşma ve Kimlik Avı: Gelen kutunuzda bir e-posta veya telefonunuzda bir mesaj bulundurun. "Hesabınızla ilgili bir sorun var ve hesabınız derhal güncellenmelidir. Tek yapmanız gereken bir bağlantıyı tıklamak." İçeriği olan bir mesaj aldığınızda, tıklamadan önce durun ve düşünün! "Kimlik avı", balık avlamak için yem kullanmaya benzer şekilde, e-postaları veya mesajları yem olarak kullanan bir sosyal mühendislik saldırısıdır. Siber saldırganlar, birinin yemi alacağı umuduyla binlerce e-posta gönderir. E-postalar bir bağlantıyı tıklamak, eki açmak veya form doldurmak gibi bir işlem yapmanızı ister. Siber saldırganlar bu e-postaları tam olarak kimin alacağından emin değiller, ancak bu görünüşte zararsız eylemlerden birini gerçekleştirmek sizi bağlayabilir. "Mızrak kimlik avı" adı verilen daha karmaşık bir kimlik avı biçimi, belirli bireyleri hedefler. Örneğin, Kuruluşumuzdaki herkes teslim edilmemiş bir paketle ilgili genel bir kimlik avı e-postası aldığında; satın alma birimimizdeki beş kişinin sahte bir fatura talebiyle hedef alınması gibi. Bir e-postanın veya iletinin kimlik avı saldırısı olup olmadığını nasıl anlarız?

Aranacak bazı işaretler:

- "Sayın Müşterimiz" veya diğer genel tebrik girişleriyle başlayan mesajlar.
- Hemen işlem yapılmasını gerektiren veya hesabınızı kapatmakla tehdit etmek gibi aciliyet duygusu yaratan mesajlar.
- Resmi bir kuruluştan geldiğini iddia eden, ancak dilbilgisi veya yazım hataları olan ya da @gmail.com, @yahoo.com veya @hotmail.com gibi kişisel bir e-posta adresi kullanan iletiler.
- Kredi kartı numaranız veya parolanız gibi son derece hassas bilgiler isteyen iletiler. Bu tür iletilerden şüphelenin. İş arkadaşınız gibi tanıdığınız biri size acil eylem

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

gerektiren bir mesaj gönderirse, sizi gönderenin gerçekten kendisi olduğunu doğrulamak için farklı kanallardan ulaşın, örneğin telefon görüşmesi yoluyla mesajın kendisine ait olup olmadığını doğrulamaya çalışın.

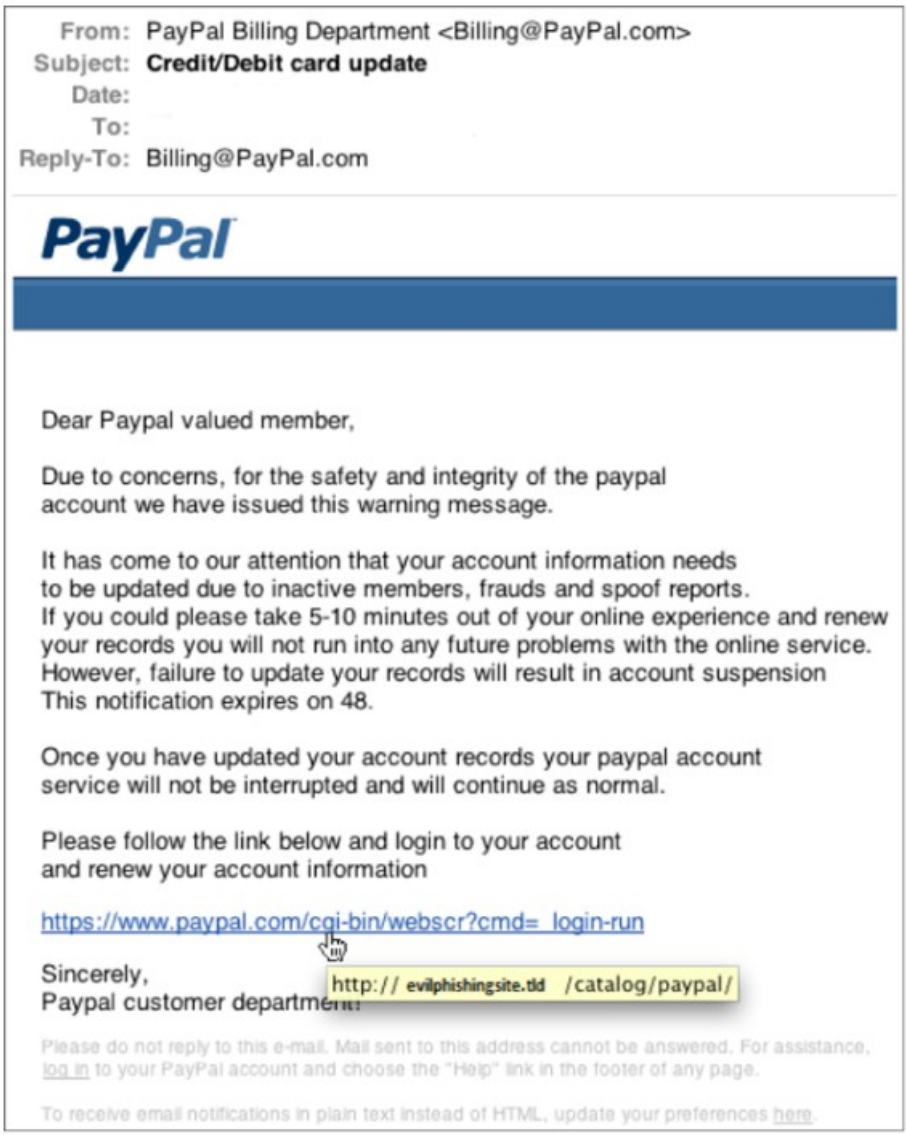
Unutmayın, bir siber saldırganın bir arkadaşınızdan veya meslektaşından gelmiş gibi görünen bir e-posta oluşturması çok kolaydır. Güvende olmak için, e-posta veya mesajlaşma kullanırken her zaman bu önlemleri almalısınız. Bir bağlantıyı tıklatmadan önce farenizi bağlantının üzerine getirin. Bu, bağlantının gerçek hedefini görüntüler, böylece meşru bir web sitesine yönlendirildiğinizi onaylayabilirsiniz. Daha da iyisi, web sitesi adresini doğrudan tarayıcınıza yazmaktır. Örneğin, bankanızdan hesap ayrıntılarını güncellemenizi isteyen bir e-posta alırsanız e-postayla gönderilen bağlantıyı yoksayın. Bankanızın web sitesi adresini tarayıcınıza yazın ve her zamanki gibi giriş yapın. İletilerin ekleri olduğunda, yalnızca beklediğiniz ekleri açın. Antivirüs çözümleri kötü amaçlı yazılımların tüm sürümlerini algılamayabileceğinden, virüslü eklere karşı sahip olduğumuz en iyi savunma sizsiniz. E-posta veya mesajlaşma kullanırken, önemli bilgileri yanlışlıkla ifşa etmemeye dikkat edin. Otomatik tamamlama gibi e-posta özellikleri, istemeden yanlış kişiye e-posta göndermeyi kolaylaştırır. Örneğin, biriminizde çalışan birine e-posta göndermek istediğinizde, yanlışlıkla başka bir birimde çalışan benzer ada sahip bir arkadaşınıza e-posta gönderebilirsiniz. Bir e-posta gönderildikten sonra kontrolünüz dışında olduğunu unutmayın.

Kimlik Avı Örnekleri

Örnek-1: Bu örnekte, e-posta PayPal.com gönderilmiş gibi görünüyor, ancak sahte bir sunucu üzerinden gönderiliyor. Yalnızca yönlendirildiği web adresine bakarsak, verilen bağlantıya tıklamadan, kimlik bilgilerini almak isteyen bir saldırgan tarafından toplanan bir e-posta olduğunu tespit edebiliriz.

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.

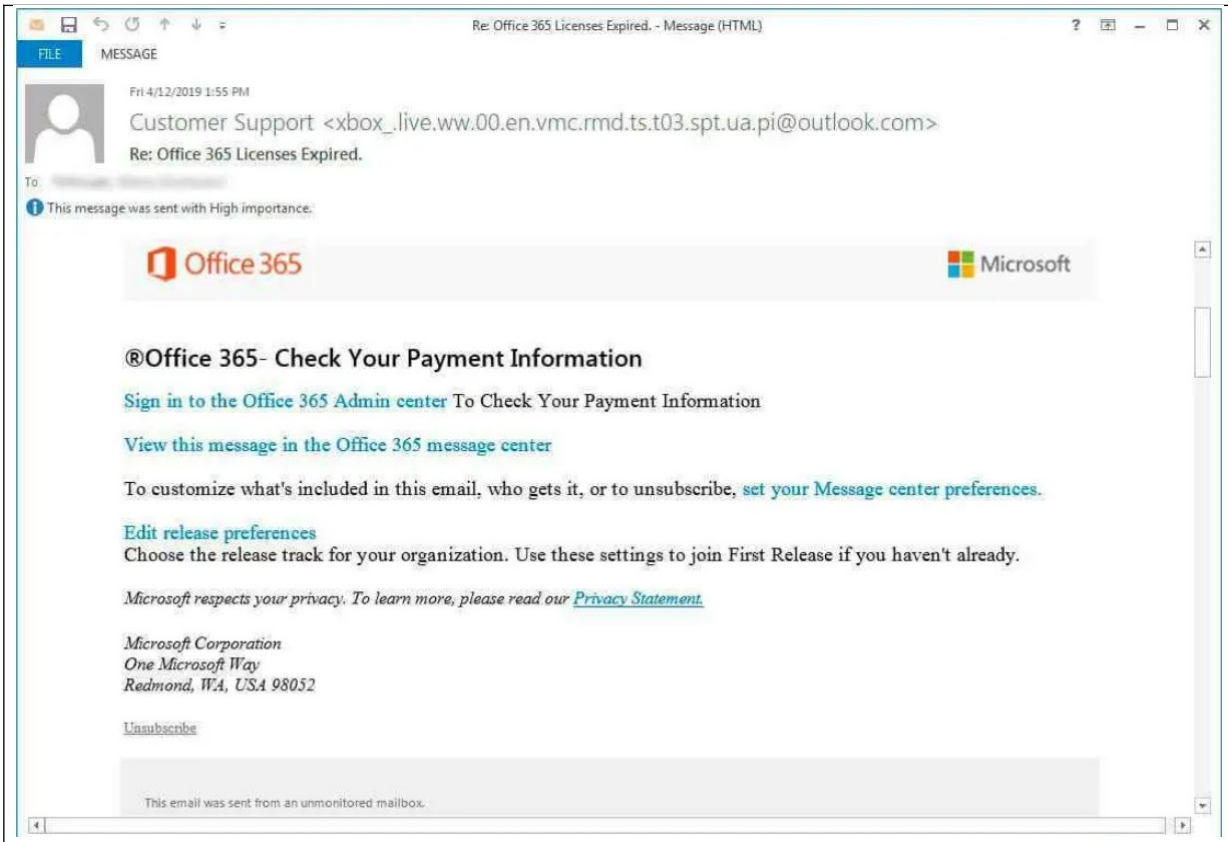
Co-funded by the Erasmus+ Programme of the European Union



Örnek-2: Bu örnekte, gelen e-posta, bir kuruluşun Office 365 lisanslarının süresinin dolduğunu gösteren bir örnektir. Posta daha sonra kullanıcıya ödeme bilgilerini denetlemek için Office 365 Yönetim Merkezi'nde oturum açmasını söylemeye devam eder.

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



Ancak gönderenin e-posta adresi dikkatle incelendiğinde böyle bir adresin bulunmayacağına dikkat edilmelidir. Kısacası, bu e-postanın Office365 tarafından gönderilmediği açıktır.

5. Sosyal ağlar

Sosyal ağ siteleri, bilgi paylaşmamıza ve başkalarıyla iletişim kurmamıza yardımcı olur. Ne yazık ki, bu siteler siber saldırganların sizi takip etmesini ve ne yaptığınızı öğrenmesini de kolaylaştırır. Her hesabı güçlü ve benzersiz bir parolayla koruyarak kendinizi koruyun. Daha da iyisi, her hesap için farklı bir şifre kullanın ve varsa iki faktörlü kimlik doğrulama kullanın. Birçok sosyal ağ sitesi üçüncü taraf uygulamalarını da destekler. Yalnızca güvenilir kaynaklardan ve yalnızca ihtiyacınız olan uygulamaları yükleyin. Herhangi bir uygulamayı yüklemeden önce uygulamanın derecelendirmesini, yorumlarını ve izinlerini kontrol edin. Artık bir uygulamaya ihtiyacınız yoksa, uygulamayı kaldırın veya sosyal ağ profilinize erişimini devre dışı bırakın.

Tıpkı e-posta ve mesajlaşma gibi, siber saldırganlar da sizi sosyal ağ sitelerinde dolandırmaya çalışabilir. Arkadaşınızmış gibi davranan mesajlar gönderebilir. Bir arkadaşınızdan garip veya şüpheli bir mesaj alırsanız, mesajı yanıtlayarak değil, e-posta veya telefon yoluyla arkadaşınızla iletişime geçin. Son olarak, Kurumumuzu korumak amacıyla, Kurumumuzla ilgili hiçbir gizli bilgiyi

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

hiçbir internet sitesinde yayınlamayın. İş hakkında neler yayınlayabileceğiniz veya paylaşabileceğiniz hakkında herhangi bir sorunuz varsa, lütfen amirinize sorun.

İki faktörlü kimlik doğrulamayı (verification) etkinleştirdikten sonra, hesabınıza yeni bir cihazdan veya tarayıcıdan her giriş yaptığınızda telefonunuza veya kimlik doğrulama uygulamanıza bir güvenlik kodu gönderilecektir. Bu kodu girmeniz gerekir ve giriş yapmanıza izin verilir. Bir siber suçlu hesabınıza giriş yapmaya çalışırsa, cep telefonunuza erişimi yoksa bunu yapamaz. Ayrıca, bir kod içeren bir bildirim alacağınız için hesabınıza giriş yapma girişimini de fark edebileceksiniz. Bu kodu asla başkalarıyla paylaşmayın! Bir saldırgan onu almaya çalışacaktır. Kodu aldıysanız ancak giriş yapmaya çalışmadıysanız, kod mesajını silin ve şifrenizi mümkün olan en kısa sürede değiştirin.

Alıştırmalar-4:

Oluşturduğunuz e-posta hesabına erişmek için iki faktörlü kimlik doğrulama gerçekleştirme gerçekleştirin. Bu işlemlerden ilki, hesaba erişmek için kullandığınız şifredir. Diğeri ise telefonunuza gönderilecek bir doğrulama kodu (SMS) veya başka bir e-posta adresine gönderilecek bir onay bağlantısı olabilir.

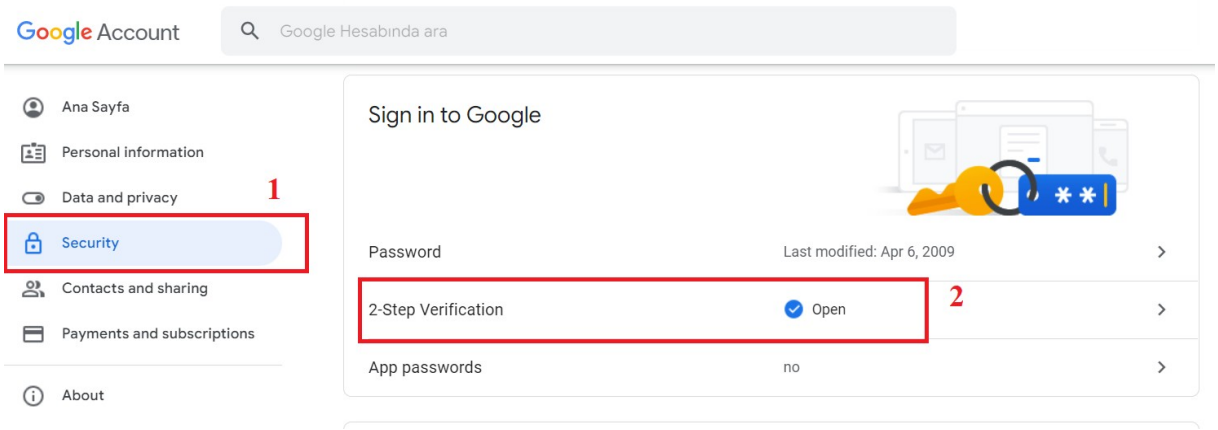
Aşağıdaki ekran görüntüsü, gmail hesabının iki faktörlü kimlik doğrulama özelliğinin nasıl etkinleştirileceğini göstermektedir.

İşlemi tamamlayın ve e-posta hesabınıza tekrar erişmeyi deneyin.

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

1. Adım: Google Hesabınızı açın.
Adım-2: " Ayarlar" bölümüne tıklayın.
Adım-3: Açılan sayfanın sol tarafındaki menüden "Güvenlik" sekmesini seçin (1). Ardından sayfanın ortasındaki "2 Adımlı Varyasyon" özelliğini etkinleştirin.



1.7. Başarılı bilgi güvenliği ilkeleri için en iyi uygulamalar

1. **Bilgi ve veri sınıflandırması:** Güvenlik programınızı oluşturabilir veya bozabilir. Kötü bilgi ve veri sınıflandırması, sistemlerinizi saldırılara açık hale getirebilir. Ek olarak, kaynakların verimsiz bir şekilde yönetilmemesi, genel giderlere neden olabilir. Açık bir sınıflandırma ilkesi, kuruluşların güvenlik varlıklarının dağıtımını kontrol altına almalarına yardımcı olur.
2. **BT operasyonları ve yönetimi:** Uyumluluk ve güvenlik gereksinimlerini karşılamak için birlikte çalışmalıdır. Departmanlar arasındaki işbirliği eksikliği yapılandırma hatalarına yol açabilir. Birlikte çalışan ekipler, riskleri azaltmak için tüm departmanlar aracılığıyla risk değerlendirmesini ve tanımlamayı koordine edebilir.
3. **Güvenlik olayı müdahale planı:** Helps, güvenlik olayları sırasında uygun düzeltme eylemlerini başlatır. Bir güvenlik olayı stratejisi, ilk tehdit yanıtını, önceliklerin tanımlanmasını ve uygun düzeltmeleri içeren bir kılavuz sağlar.
4. **SaaS ve bulut politikası** — kuruluşa, birleşik bir bulut ekosisteminin temelini oluşturabilecek net bulut ve SaaS benimseme yönergeleri sağlar. Bu politika, etkisiz komplikasyonları ve bulut kaynaklarının kötü kullanımını azaltmaya yardımcı olabilir.
5. **Kabul edilebilir kullanım politikaları (AUP'ler**): Helps, şirket kaynaklarının kötüye kullanımı nedeniyle meydana gelen veri ihlallerini önler. Şeffaf AUP'ler, tüm personelin şirket teknoloji kaynaklarının doğru kullanımı ile uyumlu kalmasına yardımcı olur.
6. **Kimlik erişimi ve yönetimi (IAM) politikası:** BT yöneticilerinin sistemleri ve uygulamaları doğru çalışanlara nasıl yetkilendirdiğini ve çalışanların güvenlik standartlarına uymak için

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

nasıl parolalar oluşturduğunu özetler. Basit bir parola ilkesi kimlik ve erişim risklerini azaltabilir.

7. **Veri güvenliği politikası:** İlgili yasa ve yönetmeliklere uymak için veri güvenliği için teknik gereklilikleri ve kabul edilebilir asgari standartları özetler
8. **Gizlilik düzenlemeleri**: Genel Veri Koruma Yönetmeliği (GDPR) gibi G'nin zorla uyguladığı düzenlemeler son kullanıcıların gizliliğini korur. Kullanıcılarının gizliliğini korumayan kuruluşlar, yetkilerini kaybetme riskiyle karşı karşıya kalır ve para cezasına çarptırılabilir.
9. **Kişisel ve mobil cihazlar politikası:** Çalışanların şirket altyapısına erişmek için kişisel cihazları kullanmasına izin verilip verilmediğini ve çalışanlara ait varlıklardan maruz kalma riskinin nasıl azaltılacağını ana hatlarıyla belirtir. Günümüzde, çoğu kuruluş buluta geçti. Çalışanlarını şirket yazılım varlıklarına herhangi bir konumdan erişmeye teşvik eden şirketler, dizüstü bilgisayarlar ve akıllı telefonlar gibi kişisel cihazlar aracılığıyla güvenlik açıkları getirme riski taşır. Kişisel cihazların uygun güvenliği için bir politika oluşturmak, çalışanlara ait varlıklar aracılığıyla tehditlere maruz kalmanın önlenmesine yardımcı olabilir.
10. **Uzaktan erişim ilkesi**: İç ağlara uzaktan bağlanmanın kabul edilebilir yöntemlerini özetler
11. **E-posta / iletişim politikası**: Çalışanların e-posta, slack veya sosyal medya gibi işletmenin seçtiği elektronik iletişim kanalını nasıl kullanabileceğini özetler
12. **Olağanüstü durum kurtarma politikası**: Kuruluşun siber güvenlik ve BT ekiplerinin genel bir iş sürekliliği planına girdilerini özetler
13. **İş sürekliliği planı (BCP):** Kuruluş genelindeki çabaları koordine eder ve bir felaket durumunda işletmeyi bir çalışma düzenine geri döndürmek için kullanılır
14. **Olay yanıtı (IR) ilkesi**: Kuruluşun bir olayı nasıl yöneteceğine ve düzelteceğine ilişkin organize bir yaklaşım
15. **Değişiklik yönetimi politikası**: BT, yazılım geliştirme ve güvenlikte değişiklik yapmak için resmi süreci ifade eder

Soru:

1- Hangisi bilgi güvenliği unsurlarından biri değildir?

A) Gizlilik

B) Dürüstlük

C) Güvenlik açığı

D) Erişilebilirlik

2- Bilgi güvenliği politikasını belirleyen kurumlardan hangisi aşağıdakilerden biri değildir?

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.

A) ENNISA

B) IPA

C) GDPR

D) NIST

3- Aşağıdaki avantajlardan hangisi bir kuruluş için doğrudan bilgi güvenliği politikalarına sahip değildir?

A) Hassas verilerin korunması

B) Güvenlik olayları riskini en aza indirmek

c) Üçüncü şahıslara açık bir güvenlik beyanı sağlamak

d) Çalışanların çalışma saatlerinin azaltılması

4- Aşağıdakilerden hangisi bilgi güvenliğine dahil değildir?

A) Donanım Politikası

B) E-posta Politikası

C) Olağanüstü Durum Kurtarma Planı Politikası

D) Parola Koruma Politikası

5- Aşağıdakilerden hangisi iyi tanımlanmış bir şifre örneği olabilir?

A) 20220829

B) InCyT # 2021!

C) Erasmus+

D) 123456!

6- Bilgi güvenliği için alınması gereken önlemlerden hangisi aşağıdakilerden biri değildir?

A) https web sayfalarını tercih edin

B) Güçlü bir şifre kullanmak

C) Kaynağı bilinmeyen bağlantıları ziyaret etmek

d) Günde en fazla 8 saat bilgisayar ekranında izlemek

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

- ***Bilgi Güvenliği Politikası Neden Önemlidir?***

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

- ***Parola Koruma İlkesi'ni açıklayınız.***

Ekler (PowerPoint sunumu, dinleyici notları, baskılar, bağlantılar, video...):

Başvuru:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/

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.