RestartVET

RESTART VET:

An innovative approach to support VET teachers/trainers through the digital transformation of VET education

Digital Security Safety (Turkish)

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

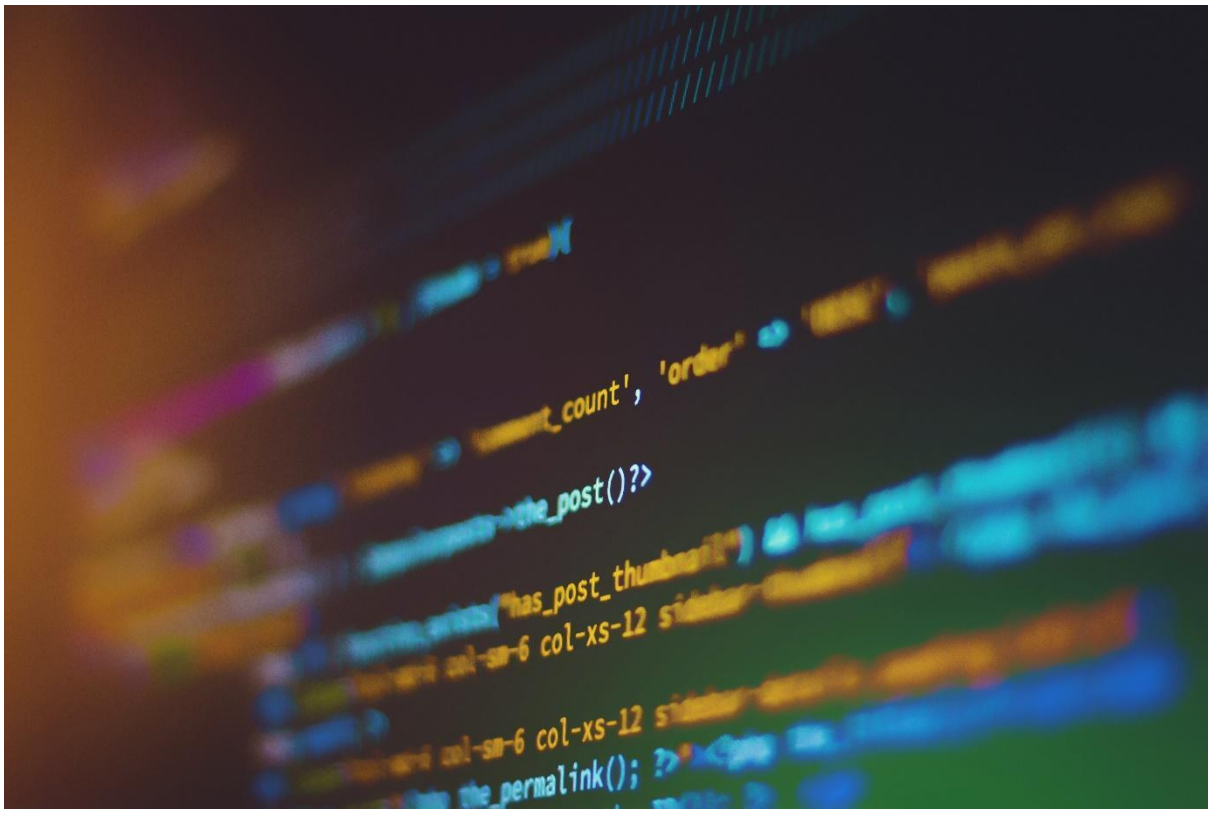
Dijital Güvenlik ve Güvenlik

Tanıtım:

Bugün günlük hayatımızın en yaygın yönlerinden bazıları, yalnızca birkaç on yıl önce bilim kurgu gibi görünürdü! Neredeyse tüm teknoloji ihtiyaçlarımız için mobil cihazların kullanımı, internetin hızı ve erişimi, uygulamaların ve BT çözümlerinin zenginliği, günlük deneyimlerimizi, ticaretimizi, eğitimimizi, eğlencemizi, araştırmamızı ve hatta kişilerarası hayatımızı yeniden şekillendirdi.

Şu anda 7,83 milyar küresel nüfus içinde dünyada 4,66 milyar aktif internet kullanıcısı olduğu tahmin ediliyor, bu da gezegendeki insanların %92,6'sının çeşitli cihazlar aracılığıyla World Wide Web'e erişimi olduğu anlamına geliyor. Yukarıdakilere ek olarak dünya nüfusunun %56,8'i de sosyal medya uygulamalarını kişisel ve profesyonel yaşamlarında düzenli olarak kullanmaktadır.

Böylesine muazzam bir teknoloji erişimiyle, dijital dünyadaki kullanıcıların güvenliğini ve güvenliğini tehlikeye atabilecek deneyimi ve tehditleri olumsuz yönde etkileyebilecek çeşitli risklerin bulunması şaşırtıcı değildir. Bu modülde, hem çevrimiçi araçların genel kullanımı hem de MEÖ sektöründeki öğrenme/öğretme yönü için dijital güvenlik ve güvenliğin başlıca yönlerini inceleyip sunacağız.



Öğrenme hedefleri:

Bu modülün sonunda şunları yapacaksınız:

- Dijital ve çevrimiçi araçların kullanımıyla ilgili riskler hakkında bilgi sahibi olmak
- dijital güvenlik ve güvenlik konusunda farkındalığı artırdı
- dijital güvenlik ve güvenlik ihtiyaçlarınızı karşılamak için temel beceriler edinmiş
- Öğrencileriniz için güvenli ve güvenli bir çevrimiçi öğrenme deneyimi sürdürmenizi sağlayacak beceriler edinmiş olmak.
- dijital güvenliği ve güvenliği korumak ve en son en iyi uygulamaları ve çözümleri benimsemek için yetkilendirilmeli ve motive edilmelidir.

Eğitmen için Genel İpuçları:

İçeriğin sorunsuz bir şekilde teslim edilmesini sağlamak için bu modülde kullanılan terimlerin ortak bir şekilde anlaşıldığından emin olun; farklı kelimeler ve farklı araçlar arasında ayrım yapmak için biraz zaman harcamak faydalı olabilir.

Öğrencilerden dijital ve çevrimiçi araçları kendi kullanımları ve bunların ne kadar kapsamlı olduğu hakkında düşünmelerini isteyin; belki onlara önümüzdeki 24 saat boyunca internet olmasaydı hayatlarının nasıl daha farklı, daha zor ve hatta daha iyi olacağını sorun.

Öğrencilerden dijital güvenlik ve emniyetle ilgili deneyimlerini veya endişelerini paylaşmalarını isteyin, bu sorunları not edin ve mümkünse bunları modülün içeriğine bağlayın. Kapsanmayan sorunlar varsa, daha fazla dış kaynak sunmaya çalışın.

1. Çevrimiçi olarak var olan başlıca tehditler/riskler nelerdir?

Reklam yazılımı (Adware)

Adware, pop-up olarak da adlandırılan, ekranınızda reklamlar oluşturmak için tasarlanmış istenmeyen yazılımlardır.

Sisteminizde reklam yazılımları olduğuna dair birkaç tipik işaret:

- Reklamlar olmaması gereken yerlerde görünür.
- Web tarayıcınızın ana sayfası, izniniz olmadan gizemli bir şekilde değişti.
- Genelde ziyaret ettiğiniz web sayfaları düzgün görüntülenmiyor.
- Web sitesi bağlantıları, beklediğinizden farklı sitelere yönlendirilir.
- Web tarayıcınız bir taramayı yavaşlatır.
- Yeni araç çubukları, uzantılar veya eklentiler aniden tarayıcınızı doldurur.
- Bilgisayarınız istenmeyen yazılım uygulamalarını otomatik olarak yüklemeye başlar.

Kötü amaçlı reklam

Kötü amaçlı reklam veya kötü amaçlı reklamcılık, dijital reklamlara kötü amaçlı kod enjekte eden bir siber saldırı tekniğidir. Hem internet kullanıcıları hem de yayıncılar tarafından tespit edilmesi zor olan bu virüslü reklamlar, genellikle meşru reklam ağları aracılığıyla tüketicilere sunulur. Reklamlar tüm web sitesi ziyaretçilerine görüntülendiğinden, hemen hemen her sayfayı görüntüleyen virüs bulaşma riski altındadır.

E-dolandırıcılık

Kimlik avı, genellikle e-posta yoluyla gönderilen ve son kullanıcıları kötü niyetli bir bağlantıya veya eke tıklamaya ikna eden saldırıdır. Saldırganlar, genellikle kötü amaçlı yazılım dağıtarak bir kuruluşta tutunmak için kimlik avı kullanabilir [1].

Oltalama Saldırısı

Hedefli kimlik avı, bir kuruluş içindeki belirli kişileri veya grupları hedefleyen bir kimlik avı yöntemidir. Kimlik avının güçlü bir çeşididir; e-postaları, sosyal medyayı, anlık mesajlaşmayı ve diğer platformları kullanarak kullanıcıların kişisel bilgilerini ifşa etmesini veya ağ güvenliğinin ihlal edilmesine, veri kaybına veya mali kayba neden olan eylemler gerçekleştirmesini sağlayan kötü niyetli bir taktiktir. Tipik bir mızraklı oltalama saldırısı, bir e-posta ve ek içerir. E-posta, hedefin adı ve şirket içindeki sıralaması da dahil olmak üzere

1

hedefe özel bilgileri içerir. Bu sosyal mühendislik taktiği, kurbanın e-postayı ve eki açmak da dahil olmak üzere enfeksiyon için gerekli tüm eylemleri gerçekleştirme şansını artırır.

Siber çömelme (Cybersquatting)

Cybersquatting, ticari markalar, hizmet markaları, şirket adları veya kişisel adlarla aynı veya benzer İnternet alan adlarının, kafa karışıklığı yaratmak veya kötü niyetli olarak kullanıcıları çekmek veya dolandırıcılık yapmak için yetkisiz olarak kaydedilmesi ve kullanılmasıdır.

Casus yazılım

Casus yazılım, bir kişi veya kuruluş hakkında bilgi toplamayı ve kullanıcıya zarar verecek şekilde başka bir varlığa göndermeyi amaçlayan kötü niyetli davranışa sahip yazılımdır.

Smishing

Smishing saldırıları, daha yaygın olarak metin mesajları olarak bilinen kısa mesaj servisini veya SMS'i kullanır.

Smishing, bankanızın temsilcisiymiş gibi davranarak sizden kişisel bilgilerinizi çalmayı, bankanızın web sayfasına bağlanmak için kısa mesajdaki bir bağlantıya tıklamanızı ve son zamanlardaki şüpheli bir ödemeyi doğrulamanızı, uygun bir şekilde müşteri hizmetleri numarasını aramanızı istemenizi içerir. Kısa süre önce şüpheli bir ödeme veya ele geçirilmiş bir hesap hakkında onlarla konuşmak için kısa mesaja dahil edilmiştir.

Yukarıdakiler, şu anda yaygın olan ve şu anda her gün milyonlarca kullanıcıyı hedefleyen çevrimiçi tehditlerin yalnızca sınırlı bir seçimini temsil etmektedir. Kullanıcıların, aşağıda "İleri Kaynaklar" başlığı altında yer alanlar gibi web sitelerini düzenli olarak izleyerek gelişmeler ve yeni tehditler hakkında bilgi sahibi olmaları tavsiye edilir:

Diğer Kaynaklar

ENISA (europa.eu)

Siber Güvenlik Riskleri | NIST

Eğitmenlerin Ek Kaynaklar listesini kendi dillerinde materyaller ve/veya ülke/bölge ile ilgili materyallerle zenginleştirmeleri tavsiye edilir. Siber güvenlik uzmanları ve araştırmacılar tarafından hazırlanan çevrimiçi makaleler ve yayınlarda da iyi bir bilgi kaynağı bulunabilir.

2. Dijital Emniyet ve Güvenlik Önlemleri

Parolalar oluşturun ve onları güçlendirin.

Çok sayıda kullanıcı, internete açık cihazların en az birinde şifre özelliğini kullanmamakta ve şifreyi kimlerin eline geçebileceklerine açık bırakmaktadır. Bilgisayarlar, tabletler ve akıllı telefonlar dahil tüm cihazlarınızı güvenli parolalarla kilitleyin. Bu, meraklı gözleri dışarıda tutacak ve cihazlarınızın kaybolması, yanlış yerleştirilmesi veya çalınması durumunda bir savunma hattı ekleyecektir. Güçlü bir parola en az 12 karakter uzunluğundadır. Güçlü parola ipuçları arasında küçük ve büyük harfler, sayılar ve simgelerden oluşan bir karışımın kullanılması ve kolayca tanımlanabilecek kişisel bilgilerin (eşin adı, evcil hayvanın adı, doğum günleri vb.) kullanılmasından kaçınılması yer alır. Zayıf bir parola, sevilen bir evcil hayvanın adı "KittkyCat" gibi herkesin kolayca öğrenebileceği bir şey olabilir; güçlü bir parola "1Kitty234Cat!!" gibi görünebilir.

Şifreleri ne sıklıkla değiştirmeniz gerekiyor?

Bir şifre ihlalinden haberdar olmadığınız sürece, her biri güçlü, benzersiz bir şifre ise şifrelerinizi düzenli olarak değiştirmenize gerek yoktur. İki faktörlü kimlik doğrulama kullanıyorsanız bu daha da doğrudur.
Mümkün olduğunda, bir tür iki faktörlü kimlik doğrulama kullanın, böylece saldırıya uğramış bir parola hesabınızın güvenliğini tehlikeye atmaz. İki faktörlü kimlik doğrulamayı makine

tarafından oluşturulan parolalarla birleştirmek, çoğu kullanıcı hesabını neredeyse kırılmaz hale getirir.

Benzersiz Parola nedir?

Benzersiz bir şifre:

1. Asla yeniden kullanılmadı. Bir kez bir şifre kullandığınızda, onu asla başka bir hesap için kullanamazsınız.
2. Yeterince uzun. Güçlü bir parola en az 12 karakter uzunluğundadır. Güçlü parola ipuçları, harf, sayı ve sembollerin bir karışımını kullanmayı içerir.
3. Seninle ilgili hiçbir şey yok. Bu, şifrenizde bir çocuğun veya evcil hayvanın adını veya size kolayca ulaşılabilecek diğer bilgileri kullanmadığınız anlamına gelir.

Kullanıcıların günümüzde birden fazla uygulama ve cihaz kullanması nedeniyle, cihazlarınızın ve uygulamalarınızın çoğu için tek bir parola kullanmak çok cazip gelebilir. Ne kadar kullanışlı olursa olsun, bu uygulama büyük bir güvenlik açığına neden olabilir, çünkü tek bir kötü niyetli saldırı hesaplarınızın çoğunu etkileyebilir ve hatta çevrimiçi bankacılık veya bulut depolama çözümlerini tehlikeye atabilir. Bu nedenle, farklı cihazlar ve uygulamalar için farklı benzersiz parolaların kullanılması şiddetle tavsiye edilir ve bu parolalar genel ağlar üzerinden paylaşılırken veya yazılırken dikkatli olunmalıdır.

İki faktörlü kimlik doğrulama nasıl çalışır?

Sosyal medya hesabınızın, e-postanızın veya diğer profillerinizin ayarlarından iki faktörlü bir doğrulamayı etkinleştirebilirsiniz. İki faktörlü kimlik doğrulama, telefon numaranızın yardımıyla veya akıllı telefonunuzdaki bir kimlik doğrulama uygulaması aracılığıyla yapılacaktır. İki faktörlü kimlik doğrulamayı etkinleştirdikten sonra, yeni bir cihazdan veya tarayıcıdan hesabınıza her giriş yaptığınızda, telefonunuza veya kimlik doğrulama uygulamanıza güvenlik kodu gönderilecektir. Bu kodu girmeniz gerekiyor ve giriş yapmanıza izin verilecek. 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 oturum açmaya çalışmadıysanız, kod mesajını silin ve şifrenizi mümkün olan en kısa sürede değiştirin.

Sosyal medyadaki gizlilik ayarları

Sosyal medyada gönderi oluştururken gizlilik ayarlarını seçebilirsiniz. Örneğin, gönderinizi hangi kitlenin göreceğini seçebilirsiniz. Bu sadece sosyal ağda eklediğiniz arkadaşlarınız olabilir, herkese açık bir gönderi olabilir veya sadece size özel bir gönderi olabilir. Ayrıca

konumunuzu belirtebilir veya belirtmeyebilirsiniz. Özel bilgilerinizin paylaşılmadığından emin olun. Örneğin, şifreleriniz, telefon numaranız, e-posta adresiniz vb.

Sosyal medya, messenger ve e-postalarda güvenlik kuralları

Sosyal ağlar, mesajlaşma programları ve e-posta yoluyla iletişimde, bahane, kötü amaçlı reklam veya farklı phishing türlerinden zarar görmemeye dikkat etmelisiniz. Tanımadığınız bir kişi tarafından size gönderilen bağlantılara tıklamayın. Dikkatli olun - siber suçlular, örneğin Facebook çalışanları veya Instagram güvenlik hizmeti gibi davranabilir. Normal bir sohbet, gönderi veya normal bir Facebook sayfasından alırsanız bu mesajlara güvenmeyin. Güvenlik mesajları size bildirimler yoluyla iletilecek veya ayarlarda mevcut olacaktır. Sosyal medya çalışanları sizden asla şifrenizi veya özel bilgilerinizi istemez.

Biri senden para mı istiyor?

Arkadaşlarınız veya aileniz acil bir durumda onlara yardım etmenizi isterse, mesajın kendilerinden geldiğini doğrulamak için her zaman onlarla kişisel olarak konuşmak için arayın. Aksi takdirde bu mesajlar siber suçlulardan gelebilir. Aile üyenizin veya bir arkadaşınızın profiliyle aynı olacak bir profil oluşturup sizden para almaya çalışabilirler.

Cihaz güvenliği

Güvenlik yazılımı kullanın. Güvenilir bir kaynaktan cihazlarınıza güvenlik yazılımı yükleyin ve güncel tutun. Virüsten koruma ve casus yazılımdan koruma yazılımını düzenli olarak çalıştırmak en iyisidir. Pop-up reklamlardan veya e-postalardan gelen güvenlik güncellemelerine karşı dikkatli olun. Aslında bilgisayarınıza bulaşabilecek kötü amaçlı yazılımlar olabilirler.

Bilgisayarınızdaki varsayılan güvenlik duvarı güvenlik korumasını kullanın. İşletim sisteminiz (OS) muhtemelen bilgisayarınızı ayarlamaya gerek kalmadan koruyacak varsayılan güvenlik duvarı ayarlarına sahiptir. Virüsten koruma yazılımınız ayrıca ayarlayabileceğiniz ek güvenlik duvarı koruması içeriyorsa, düzenli olarak kullandığınız siteleri ve programları aşırı engellemeden güvenli bir şekilde korunmanızı sağlamak için yardım için bir bilgisayar uzmanıyla iletişime geçmeyi düşünün.

Çıkış Yap. Bunları kullanmayı bitirdiğinizde uygulamalardan ve web sitelerinden çıkış yapmayı unutmayın. Bunları bilgisayar ekranınızda açık bırakmak sizi güvenlik ve gizlilik risklerine karşı savunmasız hale getirebilir.

Sizi çevrimiçi ortamda güvende tutmak için 10 ipucu

1. Parolalar oluşturun ve onları güçlendirin.

2. Hesaplarınıza güvenli erişim. Parolalar çalınabileceğinden, hesaplara iki adımlı kimlik doğrulamanın eklenmesi ikinci bir koruma katmanı sağlar. Uygulamalar ve web siteleri de dahil olmak üzere birçok çevrimiçi hizmet, bilgilerinizi korumanıza ve hesabınıza erişmeye çalışanın yalnızca sizin parolanızı bilen biri değil, gerçekten siz olduğunuzdan emin olmanıza yardımcı olabilecek ücretsiz seçenekler sunar.

3. Harekete geçmeden önce düşünün. Banka hesabınızla veya vergilerinizle ilgili bir sorun gibi aciliyet duygusu yaratan e-postalar ve iletişimler büyük olasılıkla bir dolandırıcılıktır. E-postanın yasal olup olmadığını belirlemek için doğrudan şirkete telefonla ulaşmayı düşünün.

4. Şüphe duyduğunuzda, atın. E-postalardaki bağlantılara tıklamak, genellikle dolandırıcıların kişisel bilgilere erişme şeklidir. Bir e-posta alışılmadık görünüyorsa, onu gönderen kişiyi tanıyor olsanız bile silmek en iyisidir. Dolandırıcıların arkadaşlarının e-posta adreslerine el koyabileceğini ve sana onlarmış gibi davranan mesajlar gönderebileceğini unutma. Şüpheli iletileri filtrelemeye yardımcı olması için e-posta hesabınız için spam filtrelerini açın.

5. Özenle paylaşın. Facebook gibi sosyal medya sitelerinde herkese açık olarak ne paylaştığınızın farkında olun. Bilgilerinizi kimlerin görebileceğini sınırlamak için gizlilik ayarlarınızı yapın. Konumunuzu paylaşmaktan kaçının.

6. Güvenlik yazılımı kullanın. Güvenilir bir kaynaktan cihazlarınıza güvenlik yazılımı yükleyin ve güncel tutun. Virüsten koruma ve casus yazılımdan koruma yazılımını düzenli olarak çalıştırmak en iyisidir. Pop-up reklamlardan veya e-postalardan gelen güvenlik güncellemelerine karşı dikkatli olun. Aslında bilgisayarınıza bulaşabilecek kötü amaçlı yazılımlar olabilirler.

7. Tarayıcınızın güvenlik ayarlarını yapın. Muhtemelen Firefox, Google Chrome, Internet Explorer ve Safari gibi bir internet tarayıcısı kullanarak haber, bilgi ve ürünleri ararsınız. Optimum güvenlik için seçeneklerinizi belirlemek için bu tarayıcıların her birinde ayarlarınızı yapın. Bu menüler genellikle tarayıcınızın sağ üst köşesinde bulunur. Hassas verilerden oluşan bir iz bırakmamak için oturumunuzun sonunda tarama geçmişinizi temizlemeyi düşünün.

8. Bilgisayarınızda varsayılan güvenlik duvarı güvenlik korumasını kullanın. İşletim sisteminiz (OS) muhtemelen bilgisayarınızı ayarlamaya gerek kalmadan koruyacak varsayılan güvenlik duvarı ayarlarına sahiptir. Virüsten koruma yazılımınız ayrıca ayarlayabileceğiniz ek güvenlik duvarı koruması içeriyorsa, düzenli olarak kullandığınız siteleri ve programları aşırı engellemeden güvenli bir şekilde korunmanızı sağlamak için yardım için bir bilgisayar uzmanıyla iletişime geçmeyi düşünün.

9. Oturumu kapatın. Bunları kullanmayı bitirdiğinizde uygulamalardan ve web sitelerinden çıkış yapmayı unutmayın. Bunları bilgisayar ekranınızda açık bırakmak sizi güvenlik ve gizlilik risklerine karşı savunmasız hale getirebilir.

Desteği düşünün. Dijital Güvenlik ve Güvenlik konusunda endişeleriniz varsa, güvenilir bir uzmana ulaşın veya kuruluşunuzun BT departmanı aracılığıyla destek ve içgörü isteyin.

ÖZ DEĞERLENDİRME:

- Günlük alışkanlıklarınızı ve uygulamalarınızı gözden geçirin, dijital güvenlik/güvenlik açısından savunmasız olabileceğinizi düşünüyor musunuz?
- Sunulan 10 ipucundan kaç tanesini şu anda uyguluyorsunuz?
- Kullanmayı planladığınız ipuçları veya fikirler nelerdir?
- Dijital güvenlik/güvenlik konusunda öğrencilere vereceğiniz 3 tavsiye nedir?