Proje Numarası: 2023-2-LT01-KA210-ADU-000173746

POSITIVE DIGITAL PARENTING

Ebeveynler için Pedagojiye Giriş

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. Project number 2023-2-LT01-KA210-ADU-000173746

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

GİRİŞ

UNCRC pozitif ebeveynliği; çocukların menfaatlerine ve haklarına saygı gösteren ebeveyn davranışı olarak tanımlamaktadır. İnternet, yeni dijital teknolojiler ve sosyal medyanın dünyanın dört bir yanındaki ailelere girmesiyle birlikte, ebeveynlerin temel rolü ve ebeveynliğin hedefleri değişmemiştir: ebeveynlerin hala çocuklarını beslemeleri, korumaları, ihtiyaçlarını karşılamaları, sevmeleri, onlarla bağlantı kurmaları ve onlara rehberlik etmeleri gerekmektedir. Geçmişte ve günümüzde ebeveynlik uygulamalarının, açık iletişim ve güveni teşvik eden pozitif ebeveynlik değer ve ilkelerine dayandığında en etkili olduğu da doğrudur. Geleneksel değerler ile çevrimiçi dünya arasındaki bağlantıyı kurmak ve aynı zamanda çocuklar için çevrimiçi dünya ile bağlantılı riskleri kontrol altına almak için bu modellerin ve değerlerin çevrimiçi dünyaya genişletilmesi gerekmektedir. Dijital ortam, eğitim, yaratıcılık ve sosyal etkileşim için yeni kanallar açarak çocuklar için muazzam faydalar sunmaktadır. Ancak, aynı zamanda siber zorbalık, mahremiyete yönelik riskler, diğer faaliyetlerin ihmal edilmesi, hareketsiz davranış, çevrimiçi bağımlılık gibi ciddi riskler de doğurabilir.

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

GİRİŞ

POSITIVE DIGITAL PARENTING Erasmus+ projesi, dijital medya ile etkileşime girerken, çocuklarında eleştirel düşünme becerilerini geliştirmek için ebeveynleri Medya Okuryazarlığı bilgisi ve araçları ile güçlendirmeyi amaçlamaktadır: çevrimiçi içeriği analiz etme, önyargıları tanıma, yanlış bilgileri belirleme ve dijital ortamda bilinçli kararlar verme. Eleştirel düşünmeyi medya okuryazarlığı ile birleştirerek, ebeveynler çocuklarını dijital dünyada sorumlu ve anlayışlı bir şekilde gezinmeye daha iyi hazırlayabilirler.

Bu eğitim programı, aile birimi içinde başlıca sorumlular ve eğitmenler olan ebeveynler için başlangıç eğitimi sağlayacaktır. Bu yaklaşım, ebeveynleri çevrimiçi öğrenme ve dinamik çevrimiçi araçların kullanımı ile ilgili konuları anlamaları konusunda eğitmeyi amaçlamaktadır, böylece çocuklarının dijital yaşamlarına entegre olabilirler ve ebeveynlerini ve ailelerindeki yaşlı yetişkinleri internetin tehlikeleri ve tuzakları hakkında bilgi edinmeleri için destekleyebilirler. Bu eğitim materyali çevrimiçi güvenliği teşvik etmekte ve ailenin farklı kuşakları arasında var olan dijital uçurumu ele almaktadır.

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

ORTAKLAR

ASOCİACİJA IVAIGO

- Sosyal araştırma yoluyla proje geliştirme, toplumun günümüzde karşı karşıya olduğu ana konulara odaklanma: sosyal içerme, çevresel kaygılar, her türlü ayrımcılık, dijital dönüşüm, fiziksel ve zihinsel sağlık hizmetleri, kadınların güçlendirilmesi, işsizlik, girişimcilik vb.
- Her türlü sanat ve spor aracılığıyla bilgi edinmek ve yaratıcılığı, hayal gücünü ve eleştirel düşünceyi artırmak.
- Çok kültürlü bir bağlamda katılımcıların mesleki ve kişisel becerilerinin sürdürülebilir bir şekilde geliştirilmesi.
- Gençlerin, özellikle de azınlıkların ve sosyal grupların çıkarlarının temsil edilmesi.
- Yerel faaliyetler ve uluslararası projeler aracılığıyla gençler arasında örgün ve yaygın eğitimi teşvik etmek. IVAIGO, eşitlik ve hakkaniyeti teşvik eden kapsayıcı ortamlar yaratır. that foster equity and equality.

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

ORTAKLAR

EESTI PEOPLE TO PEOPLE

Eesti People to People, 1997 yılında Estonya'da tescil edilmiş ve 1993 yılından bu yana People to People International NGO'nun bir bölümü olarak faaliyet gösteren kar amacı gütmeyen bir kuruluştur. People to People'ın amacı, farklı ülkelerden ve farklı kültürlerden insanlar arasında doğrudan fikir ve deneyim alışverişini içeren eğitimsel, kültürel ve insani faaliyetler yoluyla uluslararası anlayışı ve dostluğu geliştirmeyi amaçlamaktadır. Eesti PTP, her bir topluluk içinde ve topluluklar ve uluslar arasında kültürler arası iletişimi geliştirmeyi taahhüt eder. Hoşgörü ve karşılıklı anlayış ana temalardır.

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

ORTAKLAR

INCİRLİOVA GENCLİK KULTUR SANAT VE GELİSİM DERNEGİ

İ.ova Gençlik Kültür , Sanat ve Gelişim Derneği - IOVA kar amacı gütmeyen bir kuruluş olup, yüzün (100) üzerinde bireyi, yaratıcı vatandaşları, değerleri, fikirleri, düşünceleri, yansımaları ve vizyonu paylaşan insanları üye olarak saymaktadır. IOVA, yerel toplumun ve üyelerinin benzersiz karakteriyle ilgili fırsatları tanıyabilecek ve zorluklara yanıt verebilecek canlı, toplum temelli bir oluşuma duyulan ihtiyaca yanıt olarak kurulmuş genç ve dinamik bir kuruluştur. IOVA'nın odak noktaları aşağıdaki maddelerden oluşmaktadır :

- Yaygın eğitim yoluyla sivil katılımı ve aktif katılımı teşvik etmek;
- Medya güvenliği, sahte haberler, sosyal ağ şiddeti, medya teknolojilerinin yakınsaması vb. alanlarda yeni sosyal uygulamaların hayata geçirilmesi;
- Dijital uçurumu kapatmanın bir aracı ve AB çapında ekonomik ve sosyal kalkınma için güçlü bir araç olarak BİT stratejilerinin değeri;
- Gençlik çalışanları, yetişkin eğitmenleri ve öğretmenler için dijital eğitim sağlanması

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

İçerik

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

İnternet kullanımı, çocukların ve gençlerin çevrimiçi etkinlikleri aktif bir şekilde benimsemesi ve yaşlıların dijital ortamda yavaş bir şekilde gezinmesi ile modern aile yaşamına derinlemesine yerleşmiştir. Ebeveynler dijital ortamda yardımcı rolünü giderek daha fazla üstlendiklerinden, internet kullanımının doğasında var olan riskler konusunda dikkatli olmaları büyük önem taşımaktadır.

İnternet, bilgi ve iletişim platformlarına erişim de dahil olmak üzere çok sayıda fayda sunarken, kullanıcıları uygunsuz içerik, güvenlik ihlalleri, yanlış bilgilendirme ve siber zorbalık gibi çeşitli tehlikelere de maruz bırakmaktadır. Ebeveynler, gizliliklerine saygı gösterirken aile üyelerini proaktif olarak korumalıdır.

Ebeveynlerin dijital teknolojiye karşı cesaret kırıcı bir tutum takınmak yerine çocukların, gençlerin ve yaşlıların internetin nimetlerinden güvenli bir şekilde faydalanabilmelerini sağlama mücadelesini benimsemeleri önemlidir. Bu klavuz, onları çevrimiçi riskleri ve tehditleri belirleme ve azaltma becerileri ve bilgileriyle donatmayı içermektedir.

Bu nedenle, çocuklar, gençler, genç yetişkinler, ebeveynler ve yaşlılar dahil olmak üzere tüm aile üyeleri için kapsamlı çevrimiçi güvenlik eğitimi şarttır. Aile biriminin temel taşı olan ebeveynler, en savunmasız üyelere destek, yardım ve rehberlik sağlamak için benzersiz bir konuma sahiptir.

POSITIVE DIGITAL PARENTING Erasmus+ projesinin Güvenli Çevrimiçi Kullanım için A2 Rehberi, ebeveynleri çevrimiçi tehlikeler hakkında bilgilendirerek, aile birimlerinin güvenliğini sağlarken internet kullanımının faydalarını en üst düzeye çıkarmak için önleyici ve bilinçli bir yaklaşım benimsemelerini sağlamayı amaçlamaktadır.

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

İNTERNETTE GÜVENLİĞİN ÖNEMİ

Çevrimiçi güvenlik veya internet güvenliği, dijital dünyada sorumlu bir şekilde gezinmenin kritik bir yönüdür. Kendini ve başkalarını çevrimiçi tehdit ve tehlikelerden korumayı amaçlayan bir dizi uygulama ve davranışı kapsar. Buna kişisel bilgilerin korunması, güvenli iletişim kanallarının sağlanması ve olumlu dijital vatandaşlığın teşvik edilmesi de dahildir.

Akıllı telefonların, tabletlerin ve bilgisayarların her yerde bulunduğu günümüzün birbirine bağlı dünyasında, çevrimiçi ortamda güvende olmak her zamankinden daha fazla önem taşımaktadır. Bireyler siber zorbalık, kimlik avı dolandırıcılığı ve uygunsuz içeriğe maruz kalma gibi çevrimiçi faaliyetlerle ilişkili risklerin farkında olmalıdır. Bireyler bilgi sahibi olarak ve güvenli uygulamaları benimseyerek bu riskleri azaltabilir ve daha güvenli bir çevrimiçi deneyimin keyfini çıkarabilirler.

Ebeveynler ve bakıcılar için çocukların çevrimiçi güvenliğini sağlamak çok önemlidir. Bu, çevrimiçi etkinliklerini izlemeyi, yaşlarına uygun kısıtlamalar koymayı ve onları güvenli çevrimiçi davranış konusunda eğitmeyi içerir. Ayrıca, çevrimiçi deneyimler hakkında açık iletişimi teşvik etmek, çocukların çevrimiçi ortamda karşılaşabilecekleri endişeleri veya sorunları tartışırken daha rahat hissetmelerine yardımcı olabilir.

Nihayetinde, çevrimiçi güvenlik, bireylerin bilinçli kararlar almalarını ve dijital dünyada güvenle gezinmelerini sağlamakla ilgilidir. Uyanık kalarak ve iyi bir siber hijyen uygulayarak, hepimiz herkes için daha güvenli ve emniyetli bir çevrimiçi ortama katkıda bulunabiliriz.

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

DİJİTAL AYAK İZİ

Dijital ayak izi kavramı, internette gezinirken 'elektronik ekmek kırıntılarından' oluşan bir iz bırakmaya benzer. Bu iz, ziyaret ettiğiniz web siteleri, yüklediğiniz fotoğraflar ve sosyal ağlardaki etkileşimleriniz gibi çeşitli faaliyet ve etkileşimlerden oluşur. Sahildeki ayak izleri gibi, dijital ayak iziniz de sizin ve çevrimiçi faaliyetleriniz hakkında çok şey ortaya koyabilir.

Ancak, zamanla kaybolabilen sahilde bıraktığımız ayak izlerinin aksine, dijital ayak iziniz süresiz olarak kalabilmektedir. Bu, çevrimiçi olarak yaptığınız veya yayınladığınız her şeyin, daha sonra silseniz bile kalıcı olma potansiyeline sahip olduğu anlamına gelir. Bu kalıcılık, çevrimiçi ortamda paylaştıklarınız ve dijital eylemlerinizin olası sonuçları konusunda dikkatli olmanın önemini vurgulamaktadır.

Dijital ayak izinizde yer alan bilgiler, ilgi alanlarınız, alışkanlıklarınız ve davranışlarınız da dahil olmak üzere hakkınızda ayrıntılı bir profil oluşturmak için kullanılabilir. Bu bilgilere kimlerin erişebileceğini göz önünde bulundurmak ve sıkı gizlilik ayarlarına sahip olsanız bile, içeriğin kopyalanma ve hedef kitlenizin ötesinde paylaşılma olasılığının her zaman olduğunu anlamak çok önemlidir.

Temelde, dijital ayak izinizi yönetmek, çevrimiçi ortamda bıraktığınız izlerin farkında olmayı ve bunların niyetlerinizi ve değerlerinizi doğru bir şekilde yansıtmasını sağlamak için adımlar atmayı içerir. Bu, paylaştığınız içeriğe dikkat etmeyi, gizlilik ayarlarınızı anlamayı ve çevrimiçi eylemlerinizin potansiyel uzun vadeli sonuçlarına karşı dikkatli olmayı içerir.

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

DİJİTAL AYAK İZİ

Dijital ayak izinizi yönetmek, çevrimiçi faaliyetlerin kişisel ve profesyonel yaşamınız üzerinde uzun süreli etkilere sahip olabildiği günümüz dijital çağında çok önemlidir. İşte dijital ayak izinizi etkili bir şekilde yönetmenize yardımcı olacak bazı ipuçları:

1.Ne paylaştığınıza dikkat edin: Paylaşım yapmadan önce düşünün. Kişisel bilgilerinizi, fotoğraflarınızı veya görüşlerinizi çevrimiçi paylaşmanın olası sonuçlarını göz önünde bulundurun. Bir şey yayınlandıktan sonra tamamen kaldırmanın zor olabileceğini unutmayın.

2. Gizlilik ayarlarını kullanın: Sosyal medya platformlarındaki ve diğer çevrimiçi hizmetlerdeki gizlilik ayarlarına aşina olun. Gönderilerinizi ve bilgilerinizi kimlerin görebileceğini kontrol etmek için bu ayarları yapın.

3.Çevrimiçi varlığınızı düzenli olarak gözden geçirin: Sosyal medya profillerinizi ve çevrimiçi hesaplarınızı periyodik olarak gözden geçirin. Güncel olmayan veya ilgisiz bilgileri kaldırın veya güncelleyin.

4.Kişisel bilgileri sınırlayın: Adresiniz, telefon numaranız veya finansal bilgileriniz gibi hassas kişisel bilgilerinizi çevrimiçi ortamda paylaşmaktan kaçının.

5.Güçlü parolalar kullanın: Yetkisiz erişimi önlemek için çevrimiçi hesaplarınız için güçlü, benzersiz parolalar kullanın. Şifrelerinizi güvenli bir şekilde takip etmek için bir şifre yöneticisi kullanmayı düşünün.

6.Neye tıkladığınıza dikkat edin: Kimlik avı dolandırıcılıklarına ve kötü niyetli bağlantılara karşı dikkatli olun. Bilinmeyen veya şüpheli kaynaklardan gelen bağlantılara tıklamaktan veya ekleri indirmekten kaçının.

7.Çevrimiçi tanınırlığınızı izleyin: Hakkınızda çevrimiçi olarak hangi bilgilerin mevcut olduğunu düzenli olarak kontrol etmek için arama motorlarını kullanın. Yanlış veya zararlı bir bilgi bulursanız, bunu gidermek için adımlar atın.

8.Kendinizi ve başkalarını eğitin: Çevrimiçi güvenlik ve gizlilik için en iyi uygulamalar hakkında bilgi sahibi olun. Arkadaşlarınızı ve ailenizi dijital ayak izlerini yönetmenin önemi konusunda eğitin.

Bu ipuçlarını takip ederek dijital ayak izinizi etkili bir şekilde yönetebilir ve çevrimiçi itibarınızı koruyabilirsiniz. Çevrimiçi varlığınızın sizin bir yansımanız olduğunu unutmayın, bu nedenle ne paylaştığınızı ve kendinizi çevrimiçi olarak nasıl sunduğunuzu kontrol etmeniz çok önemlidir.

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

ÇEVRİMİÇİ GİZLİLİK

İnternet gizliliği veya dijital gizlilik olarak da bilinen çevrimiçi gizlilik, bir kişi çevrimiçi olduğunda kişisel, finansal ve tarama bilgilerinin ne ölçüde gizli kaldığıdır. Çevrimiçi ortamda paylaşılan ve depolanan kişisel veri miktarının artmasıyla birlikte, çevrimiçi gizlilikle ilgili endişeler önemli ölçüde artmıştır.

Çevrimiçi gizliliğin korunması çeşitli nedenlerden dolayı çok önemlidir. Öncelikle, bireyler kişisel yaşamlarının ayrıntılarını gizli tutma ve bunları yabancılarla paylaşmama hakkına sahiptir. Ayrıca, bir şirket tarafından toplanan veriler bilginiz veya izniniz olmadan başkalarıyla paylaşılabileceğinden, hangi kişisel bilgilerin kim tarafından toplandığını bilmek zor olabilir.

Çevrimiçi veri gizliliği, tıpkı dünyadaki gizlilik gibi aynı önem seviyesinde ele alınmalıdır. Tıpkı kapalı kapılar ardında gizli bir konuşma yaptığınız veya finansal bilgilerinizi yalnızca bir banka ile paylaştığınız gibi, çevrimiçi gizliliğinizi korumak için adımlar atmalısınız. Bu, güçlü ve benzersiz şifreler kullanmayı, çevrimiçi paylaştığınız bilgiler konusunda dikkatli olmayı ve sosyal medya ve diğer çevrimiçi platformlardaki gizlilik ayarlarınızı düzenli olarak gözden geçirmeyi içerir.

Çevrimiçi gizliliğinize değer vererek ve koruyarak, kişisel bilgilerinizin kötüye kullanılması veya izniniz olmadan paylaşılması riskini azaltabilirsiniz.

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

VERİ GİZLİLİĞİ

Veri gizliliği, özellikle Avrupa Birliği'nde Genel Veri Koruma Yönetmeliği'nin (GDPR) uygulanmasıyla birlikte büyük ilgi gören temel bir haktır. 2018 yılında yürürlüğe giren GDPR, kişisel verilerin nasıl toplandığı, işlendiği ve saklandığına ilişkin katı kurallar getirerek her AB vatandaşının gizliliğini ve verilerini korumak üzere tasarlanmıştır.

GDPR, veri korumanın çeşitli yönlerini özetleyen 99 maddeden oluşmaktadır. Bazı temel hükümler şunlardır:

1. Erişim hakkı: Bireyler, bir şirketin kendileri hakkında hangi verileri tuttuğunu ve bunların nasıl kullanıldığını bilme hakkına sahiptir.

2.Silme hakkı: "Unutulma hakkı" olarak da bilinen bu hak kapsamında bireyler, belirli koşullar altında kişisel verilerinin silinmesini talep edebilir.

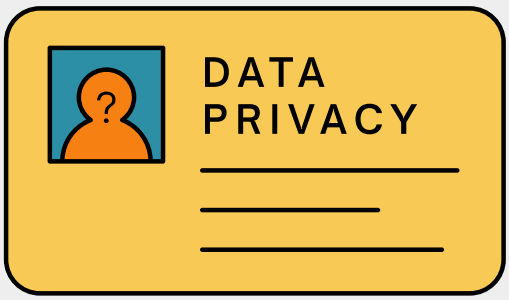
3.Rıza: Şirketler, kişisel verilerini toplamadan veya işlemeden önce bireylerden açık rıza almalıdır. Bu, çerezler ve tarama geçmişi için açık ve net rızayı içerir.

4.Veri minimizasyonu: Şirketler yalnızca toplanma amacı için gerekli olan verileri toplamalı ve işlemelidir.

5.Veri taşınabilirliği: Bireyler, kişisel verilerini bir şirketten yaygın olarak kullanılan ve makine tarafından okunabilir bir formatta alma hakkına sahiptir.

6.Veri koruma görevlileri: Bazı kuruluşların GDPR uyumluluğunu denetlemek için bir Veri Koruma Görevlisi ataması gerekmektedir.

GDPR, şirketlerin kişisel verileri nasıl ele aldıklarını önemli ölçüde etkileyerek daha katı veri koruma önlemleri uygulamalarını ve veri işleme uygulamalarına ilişkin daha fazla şeffaflık sağlamalarını gerektirmiştir. GDPR, veri gizliliği haklarının geliştirilmesinde ve bireylerin kişisel bilgileri üzerinde daha fazla kontrol sahibi olmalarının sağlanmasında etkili olmuştur.



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

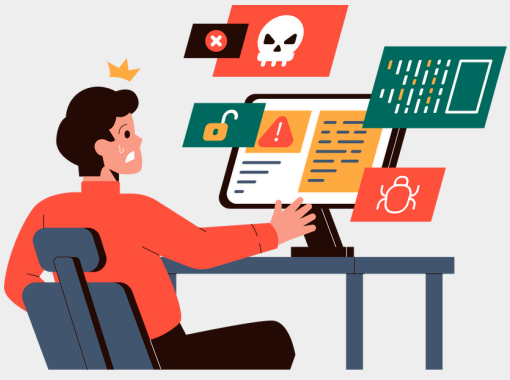
ÇEVRİMİÇİ TEHDİTLER

Siber tehditler, verilere zarar vermeyi, bilgi çalmayı veya dijital operasyonları aksatmayı amaçlayan kötü niyetli faaliyetlerdir. Bu tehditler, bilgi teknolojisi varlıklarını, bilgisayar ağlarını, fikri mülkiyeti ve hassas verileri hedef alan siber saldırılar da dahil olmak üzere çok çeşitli eylemleri kapsar. Siber tehditler hem iç hem de dış kaynaklardan kaynaklanabilir.

İç tehditler, bir kuruluş içindeki ayrıcalıklarını veya hassas bilgilere erişimlerini kötüye kullanan güvenilir kullanıcılardan kaynaklanabilir. Öte yandan, dış tehditler uzak konumlardan kaynaklanır ve genellikle dijital sistemlerdeki güvenlik açıklarından yararlanmak isteyen bilinmeyen taraflarca gerçekleştirilir.

Siber tehditlere örnek olarak kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı saldırıları ve hizmet reddi (DoS) saldırıları verilebilir. Bu tehditlerin mali kayıplar, veri ihlalleri ve bir kuruluşun itibarına zarar vermek gibi ciddi sonuçları olabilir.

Siber tehditlere karşı korunmak için kuruluşlar ve bireyler sağlam siber güvenlik önlemleri almalıdır. Bu önlemler arasında yazılımların düzenli olarak güncellenmesi, güçlü parolaların kullanılması, hassas verilerin şifrelenmesi ve kullanıcıların olası tehditler ve bunlardan nasıl kaçınılacağı konusunda eğitilmesi yer alır. Ayrıca, çok faktörlü kimlik doğrulamanın uygulanması ve verilerin düzenli olarak yedeklenmesi bir siber saldırının etkisini azaltmaya yardımcı olabilir.



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

ÇEVRİMİÇİ TEHLİKELER

İnternet tehlikeleri, bir internet kullanıcısına zarar verebilecek her şey olarak tanımlanabilir. Bu zarar birçok şekilde olabilir (örneğin, fiziksel, duygusal, psikolojik, finansal, sosyal ve itibarla ilgili). Farklı türdeki internet tehlikelerinin birçoğu aşağıda özetlenmiştir:

Çevrimiçi tehlikelerin türleri:
Günümüzde internet üzerinden eğlence, kredi ve finansal hizmetlerden dünyanın her köşesinden ürünlere kadar hemen her şeye erişme imkanı bulunmaktadır. İnternet belirli bir düzeyde anonimlik sağlarken, kullanıcının kişisel bilgilerinin risk altında olabileceği yollar giderek artmaktadır.

1-Siber Zorbalık: Siber zorbalık, sosyal medya, mesajlaşma platformları, oyun platformları ve cep telefonları gibi dijital teknolojiler kullanılarak gerçekleştirilen bir zorbalık türüdür. Hedef alınan bireyi korkutmayı, kızdırmayı veya utandırmayı amaçlayan tekrarlanan davranışları içerir. Siber zorbalık örnekleri arasında sosyal medyada biri hakkında yalanlar veya söylentiler yaymak, mesajlaşma uygulamaları aracılığıyla incitici mesajlar veya tehditler göndermek ve kötü mesajlar göndermek için birinin kimliğine bürünmek yer alır.

Yüz yüze zorbalık ile siber zorbalık arasındaki en önemli farklardan biri, siber zorbalığın dijital bir ayak izi bırakmasıdır. Bu, zorbalık davranışının bir kaydı olduğu anlamına gelir ve bu da istismarı durdurmak için kanıt sağlamada yararlı olabilir. Bireylerin dijital ayak izlerinin farkında olmaları ve çevrimiçi eylemlerinin gerçek dünyada sonuçları olabileceğini anlamaları önemlidir.

Siber zorbalıkla mücadele etmek için, bireylerin her türlü siber zorbalık vakasını ilgili platforma veya yetkiliye bildirmeleri çok önemlidir. Gençleri sorumlu çevrimiçi davranış ve siber zorbalığın etkileri konusunda eğitmek de önemlidir. Birlikte çalışarak herkes için daha güvenli bir çevrimiçi ortam yaratabiliriz.

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

ÇEVRİMİÇİ TEHLİKELER

2- Siber Avcılar : Siber Avcı, çocukları ve gençleri cinsel, duygusal, psikolojik veya finansal zarar da dahil olmak üzere çeşitli istismar biçimleri için sömürmek üzere interneti kullanan, genellikle yetişkin olan bir kişidir. Bu avcılar, sohbet odaları, anlık mesajlaşma, sosyal ağlar ve video oyunları gibi çeşitli çevrimiçi platformlar aracılığıyla savunmasız bireyleri hedef alır.

Siber Avcıların kullandığı yaygın taktiklerden biri, sahte bir kimlik oluşturarak kendilerini çocuk veya genç gibi göstermektir. Bu sahte kimliği, kurbanlarıyla ilişki kurmak, yavaş yavaş güvenlerini kazanmak ve onları zararlı faaliyetlere katılmaya yönlendirmek için kullanırlar.

Tımar süreci, Siber Avcıların kullandığı önemli bir stratejidir; burada kurbanlarını zaman içinde yavaşça manipüle ederler ve genellikle onların zayıflıklarını ve güvensizliklerini istismar ederler. Bu süreç, mağduru kendi çıkarları için istismar etmeden önce onunla görünüşte gerçek bir arkadaşlık veya ilişki kurmayı içerebilir.

Ebeveynlerin, bakıcıların ve eğitimcilerin çocukları ve gençleri çevrimiçi güvenlik ve Siber Avcıların yarattığı tehlikeler konusunda eğitmeleri çok önemlidir. Çevrimiçi etkileşimler hakkında açık iletişimi teşvik etmek ve sınırları belirlemek, gençleri bu avcıların kurbanı olmaktan korumaya yardımcı olabilir. Ayrıca, çevrimiçi faaliyetlerin izlenmesi ve uyarı işaretlerinin farkında olunması, potansiyel istismarın tespit edilmesine ve önlenmesine yardımcı olabilir.

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

ÇEVRİMİÇİ TEHLİKELER

3-Özel Bilgileri Paylaşmak Kişisel bilgileri paylaşmaktan kaçınmak, verileri korumak, kimlik hırsızlığını önlemek ve çevrimiçi ortamda güvende kalmak için çok önemlidir. Bu sadece internette gezinirken değil, aynı zamanda sosyal medya platformlarında bilgi kullanırken ve paylaşırken de önemlidir.

Korunması gereken kişisel bilgi örnekleri şunlardır:
1. İsimler: Tam ad, aile adı ve ebeveyn adları.
2. Kişisel kimlik numaraları: Sosyal güvenlik numarası, ehliyet numarası, pasaport numarası, hasta kimlik numarası, vergi mükellefi kimlik numarası, kredi hesap numarası veya finansal hesap numarası.
3. Adresler: Sokak adresi ve e-posta adresi.
4. Biyometri: Retina taramaları, parmak izleri, yüz geometrisi veya sesli imzalar.
5. Araç kimliği veya başlık numaraları.
6. Telefon numaraları.
7. Teknoloji varlık bilgileri: Belirli bir kişiye bağlı Medya Erişim Kontrolü (MAC) veya İnternet Protokolü (IP) adresleri.

Sosyal medyayı kullanırken, paylaştığınız bilgilere dikkat etmeniz önemlidir. Tam adınız, adresiniz veya telefon numaranız gibi kişisel bilgilerinizi herkese açık olarak paylaşmaktan kaçının. Gönderilerinizi ve bilgilerinizi kimlerin görebileceğini kontrol etmek için gizlilik ayarlarını kullanın ve tanımadığınız kişilerden gelen arkadaşlık isteklerini veya mesajları kabul etme konusunda dikkatli olun. Kişisel bilgilerinizi koruma konusunda dikkatli davranarak kimlik hırsızlığı ve diğer çevrimiçi tehdit risklerini azaltabilirsiniz.

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

ÇEVRİMİÇİ TEHLİKELER

4- Oltalama: Oltalama saldırıları, siber suçlular tarafından bireyleri kredi kartı numaraları veya oturum açma kimlik bilgileri gibi hassas bilgileri vermeleri için kandırmak amacıyla kullanılan aldatıcı taktiklerdir. Bu saldırılar genellikle meşru kaynaklardan geliyormuş gibi görünen e-postalar veya mesajlar gibi sahte iletişimleri içerir. Oltalama saldırılarının amacı kişisel bilgileri çalmak veya kurbanın cihazına kötü amaçlı yazılım yüklemektir.

Kimlik avı saldırıları, bankanızdan veya popüler bir web hizmetinden geliyormuş gibi görünen e-postalar da dahil olmak üzere çeşitli şekillerde olabilir. Bu e-postalar genellikle tıklandığında meşru sitenin görünümünü taklit eden sahte web sitelerine yönlendiren bağlantılar içerir. Sahte web sitesine girdikten sonra, kurbanlardan kişisel bilgilerini girmeleri istenir ve bu bilgiler siber suçlular tarafından ele geçirilir.

Kimlik avı saldırıları geleneksel olarak e-postalarla ilişkilendirilse de, siber suçlular artık kurbanları hedef almak için başka yöntemler de kullanıyor. Bunlar arasında kısa mesajlar, telefon aramaları, sahte uygulamalar ve sosyal medya testleri yer almaktadır. Bu taktikler, bireyleri kişisel bilgilerini vermeye veya kötü amaçlı bağlantılara tıklamaya ikna etmek için tasarlanmıştır.

Kimlik avı saldırılarına karşı korunmak için, bilinmeyen gönderenlerden gelen e-postaları veya mesajları açarken dikkatli olmak önemlidir. Gönderenin e-posta adresini kontrol ederek ve şüpheli kaynaklardan gelen bağlantılara tıklamaktan veya ekleri indirmekten kaçınarak e-postaların gerçekliğini doğrulayın. Ayrıca, kimlik avı saldırılarını tespit etmeye ve önlemeye yardımcı olması için güvenlik yazılımı kullanın ve güncel tutun

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

ÇEVRİMİÇİ TEHLİKELER

5-Dolandırıcılığa Kanmak: İnternet dolandırıcılığı, siber suçlular tarafından internette yürütülen dolandırıcılık planlarıdır. Bu dolandırıcılıklar çeşitli şekillerde olabilir ve bireyleri hassas bilgiler veya para vermeleri için kandırmak üzere tasarlanmıştır. İnternet dolandırıcılığı, kimlik avı e-postaları, sosyal medya, SMS mesajları, sahte teknik destek telefon aramaları ve korkutucu yazılımlar gibi çeşitli kanallar aracılığıyla gerçekleşebilir.
İnternet dolandırıcılığının ana hedefi genellikle kredi kartı bilgileri veya oturum açma bilgileri gibi kişisel bilgileri çalmak veya bireyleri dolandırıcıya para göndermeleri için kandırmaktır. Bazı yaygın internet dolandırıcılığı türleri şunlardır:

1. Kimlik avı e-postaları: Bankalar veya devlet kurumları gibi yasal kuruluşlardan geliyormuş gibi görünen, ancak aslında bireyleri kişisel bilgilerini vermeleri veya kötü amaçlı bağlantılara tıklamaları için kandırmaya çalışan e-postalar.

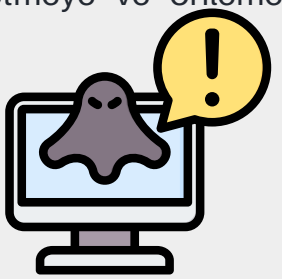
2.Sosyal medya dolandırıcılığı: Kimlik avı web sitelerine veya kötü amaçlı yazılım indirmelerine yönlendiren sahte profiller veya reklamlar gibi sosyal medya platformlarında meydana gelen dolandırıcılıklar.

3.SMS dolandırıcılığı: Kısa mesaj yoluyla gönderilen, genellikle sahte web sitelerine bağlantılar veya kişisel bilgi talepleri içeren dolandırıcılıklar.

4. Sahte teknik destek aramaları: Bireyleri bilgisayarlarında bir sorun olduğuna ikna etmeye çalışan ve ardından sorunu "düzeltmek" için ödeme veya bilgisayara erişim talep eden teknik destek temsilcileri gibi davranan dolandırıcılar.

5. Scareware: Bir bilgisayara virüs bulaştığını iddia eden ve kullanıcıdan gereksiz yazılım veya hizmetler satın almasını isteyen sahte yazılımlar veya açılır mesajlar.

İnternet dolandırıcılığına karşı korunmak için, istenmeyen mesajlar veya kişisel bilgi talepleri alırken dikkatli olmak önemlidir. Herhangi bir bilgi vermeden veya bağlantılara tıklamadan önce gönderenin veya kuruluşun meşruiyetini doğrulayın. Ayrıca, dolandırıcılıkları tespit etmeye ve önlemeye yardımcı olmak için güncel güvenlik yazılımları kullanın.



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

ÇEVRİMİÇİ TEHLİKELER

6-Kazara kötü amaçlı yazılım indirmek: Yanlışlıkla kötü amaçlı yazılım indirmek, ciddi sonuçlar doğurabilecek yaygın bir bilgisayar güvenliği tehdididir. Kötü amaçlı yazılımın kısaltması olan malware, bilgisayar sisteminize zarar vermek veya sisteminizi bozmak için tasarlanmış virüsleri, solucanları, Truva atlarını ve diğer zararlı programları içerir.

Bilgisayar virüsü, kendini kopyalayabilen ve diğer bilgisayarlara yayılabilen bir kötü amaçlı yazılım türüdür. Genellikle bilginiz veya izniniz olmadan bilgisayarınızın çalışma şeklini değiştirebilir ve küçük rahatsızlıklardan ciddi hasara kadar bir dizi soruna neden olabilir.

Yanlışlıkla kötü amaçlı yazılım indirmekten kaçınmak için internetten yazılım indirirken dikkatli olmak önemlidir. Ücretsiz yazılımları dikkatlice değerlendirin ve eşler arası dosya paylaşım sitelerinden indirmekten kaçının, çünkü bunlar yaygın kötü amaçlı yazılım kaynaklarıdır. Ayrıca, kötü amaçlı ekler veya bağlantılar içerebilecekleri için bilinmeyen gönderenlerden gelen e-postalara karşı dikkatli olun.

Günümüzde çoğu web tarayıcısı, çevrimiçi tehditlere karşı korunmaya yardımcı olabilecek yerleşik güvenlik ayarlarına sahiptir. Bu ayarları güncel tutmak ve açılır pencere engelleyicileri ve kimlik avı önleme araçları gibi ek güvenlik özelliklerini etkinleştirmek önemlidir.
Bununla birlikte, virüslere ve diğer kötü amaçlı yazılımlara karşı korunmanın en etkili yolu, saygın bir sağlayıcıdan alınan güncel bir antivirüs yazılımı kullanmaktır. Antivirüs yazılımı bilgisayarınızdaki kötü amaçlı yazılımların tespit edilip kaldırılmasına yardımcı olmanın yanı sıra yeni tehditlere karşı gerçek zamanlı koruma da sağlayabilir. Antivirüs yazılımınızı düzenli olarak güncellemek ve bilgisayarınızı taramak, sisteminizi kötü amaçlı yazılım bulaşmalarına karşı güvende tutmanıza yardımcı olabilir.

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

ÇEVRİMİÇİ ORTAMDA GÜVENDE OLMAK İÇİN TEMEL YETKİNLİKLER

Çevrimiçi güvenlik, internete bağlı herhangi bir cihazı kullanırken çocukların, gençlerin ve ailenin daha savunmasız üyelerinin güvenliğini teşvik etmek için kullanılan genel bir kelimedir. Çevrimiçi dünya, çocukların ve gençlerin hayatlarını hem kişisel hem de eğitimsel olarak çeşitli şekillerde zenginleştirebilir.
Öğrencilerin çevrimiçi ortamda güvende kalmaları için temel yeterlilikleri özetlemek önemlidir:

a. Risklerin farkına varmak: Çevrimiçi faaliyetin risklerini tanımak, internette güvende kalmak için çok önemlidir. Potansiyel tehdit ve tehlikeleri belirleyerek, bireyler çevrimiçi maruziyetlerini azaltmak ve kendilerini zarardan korumak için proaktif adımlar atabilirler.

Başlangıç olarak, çevrimiçi güvenlik için önleyici bir yaklaşım benimsemek önemlidir. Bu, potansiyel risklerin farkında olmak ve bir sorun haline gelmeden önce bunları azaltmak için adımlar atmak anlamına gelir. Kimlik avı dolandırıcılığı, kötü amaçlı yazılım ve kimlik hırsızlığı gibi yaygın çevrimiçi tehditler hakkında bilgi sahibi olarak bireyler kendilerini bu tehlikelerden daha iyi koruyabilirler.

Çevrimiçi maruziyeti azaltmak, çevrimiçi güvende kalmanın bir diğer önemli yönüdür. Bu, sosyal medyada ve diğer web sitelerinde paylaşılan kişisel bilgi miktarını sınırlamayı, bilgilerinizi kimlerin görebileceğini kontrol etmek için gizlilik ayarlarını kullanmayı ve bilinmeyen kaynaklardan gelen bağlantılara tıklama veya ekleri indirme konusunda dikkatli olmayı içerebilir.

Çevrimiçi faaliyetlerin risklerini tanımak ve maruziyeti azaltmak için proaktif adımlar atmak, dijital dünyada güvende ve emniyette kalmak için çok önemlidir. Bireyler bilgi sahibi olarak ve proaktif davranarak kendilerini çevrimiçi tehditlerden koruyabilir ve daha güvenli bir çevrimiçi deneyimin keyfini çıkarabilirler.

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

ÇEVRİMİÇİ ORTAMDA GÜVENDE OLMAK İÇİN TEMEL YETKİNLİKLER

b.Kişisel bilgileri güvende tutun:
Kişisel bilgileri güvende tutmak, güvenli bir çevrimiçi varlık sürdürmek için çok önemlidir. Kimliğinizi korumak ve siz ve aileniz için güvenli bir dijital yaşam sağlamak için belirli yönergeleri takip etmek önemlidir:

1.Güçlü, benzersiz parolalar kullanın: Parolalar dijital evinizin anahtarlarıdır. Her bir hesabınız için güçlü, benzersiz parolalar kullanmanız ve kolayca tahmin edilebilen parolalar kullanmaktan kaçınmanız çok önemlidir. Karmaşık parolaları güvenli bir şekilde oluşturmak ve saklamak için saygın bir parola yöneticisi kullanmayı düşünün.

2. Şifreleri paylaşmaktan kaçının: Şifrelerinizi asla kimseyle, güvenilir kişilerle bile paylaşmayın. Şifrelerin paylaşılması hesaplarınızın ve kişisel bilgilerinizin güvenliğini tehlikeye atabilir.

3.Verilerinizi yedekleyin: Önemli verilerinizi kaybolmaya veya çalınmaya karşı korumak için düzenli olarak yedekleyin. Bu işlem harici sabit diskler, bulut depolama hizmetleri veya diğer yedekleme çözümleri kullanılarak yapılabilir. Yedekleme verileri şifrelenmeli ve güvenli bir şekilde saklanmalıdır.

4.Yazılımları güncel tutun: İşletim sistemleri, tarayıcılar ve uygulamalar dahil olmak üzere cihazlarınızdaki tüm yazılımların en son güvenlik yamaları ve güncellemeleri ile düzenli olarak güncellendiğinden emin olun. Bu, siber suçlular tarafından istismar edilebilecek güvenlik açıklarına karşı korunmaya yardımcı olur.

5.Güvenlik yazılımı kullanın: Virüslere, kötü amaçlı yazılımlara ve diğer çevrimiçi tehditlere karşı korunmak için cihazlarınıza saygın antivirüs ve kötü amaçlı yazılımdan koruma yazılımı yükleyin ve düzenli olarak güncelleyin.

6.İki faktörlü kimlik doğrulamayı (2FA) etkinleştirin: Ekstra bir güvenlik katmanı eklemek için mümkün olduğunda hesaplarınızda 2FA'yı etkinleştirin. Bu, şifrenize ek olarak telefonunuza gönderilen bir kod gibi ikinci bir doğrulama şekli gerektirir.

Bu yönergeleri izleyerek kişisel bilgilerinizi korumaya yardımcı olabilir ve siz ve aileniz için daha güvenli bir çevrimiçi deneyim sağlayabilirsiniz.

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

ÇEVRİMİÇİ ORTAMDA GÜVENDE OLMAK İÇİN TEMEL YETKİNLİKLER

c.Bilinmeyen dosyaları indirmeyin: Bilinmeyen dosyaların indirilmesi bilgisayarınızı ve kişisel bilgilerinizi kötü amaçlı yazılımlar, virüsler ve diğer kötü amaçlı yazılımlar dahil olmak üzere çeşitli risklere maruz bırakabilir. Kendinizi ve cihazlarınızı korumak için bu yönergelere uymanız önemlidir:

1.E-posta eklerine karşı dikkatli olun: Bilinmeyen veya şüpheli e-postalardan gelen ekleri indirmeyin. Bu ekler bilgisayarınıza zarar verebilecek veya kişisel bilgilerinizi çalabilecek kötü amaçlı yazılımlar içerebilir.

2.Kaynağı doğrulayın: Herhangi bir dosyayı indirmeden önce, meşru olduğundan emin olmak için kaynağı doğrulayın. Yalnızca güvenilir web sitelerinden ve kaynaklardan dosya indirin.

3. Güvenilir antivirüs yazılımları kullanın: Bilgisayarınıza antivirüs yazılımı yükleyin ve düzenli olarak güncelleyin. Bu yazılım, indirilen dosyalardaki kötü amaçlı yazılımların tespit edilmesine ve kaldırılmasına yardımcı olabilir.

4.Dosya uzantılarını etkinleştirin: İşletim sisteminizde dosya uzantılarını etkinleştirin, böylece tam dosya adını görebilirsiniz. Bu, potansiyel olarak zararlı dosyaları belirlemenize yardımcı olabilir.

5.Eşler arası (P2P) dosya paylaşımından kaçının: P2P dosya paylaşım hizmetlerini kullanırken dikkatli olun, çünkü sizi kötü amaçlı yazılımlara ve diğer risklere maruz bırakabilirler. Dosyaları yalnızca güvenilir kaynaklardan indirin.

6. Açmadan önce dosyaları tarayın: İndirilen dosyaları açmadan önce taramak için antivirüs yazılımı kullanın. Bu, dosyada bulunan herhangi bir kötü amaçlı yazılım veya virüsün tespit edilmesine yardımcı olabilir.

Bu yönergeleri izleyerek, bilinmeyen dosyaları indirme riskini azaltabilir ve bilgisayarınızı ve kişisel bilgilerinizi çevrimiçi tehditlerden koruyabilirsiniz.

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

ÇEVRİMİÇİ ORTAMDA GÜVENDE OLMAK İÇİN TEMEL YETKİNLİKLER

d. Çevrimiçi bilgileri analiz etmek ve değerlendirmek için eleştirel düşünme becerilerini kullanın;
Çevrimiçi bilgileri analiz etmek ve değerlendirmek için eleştirel düşünme becerilerini kullanmak, kendinizi dolandırıcılıklardan, kimlik avı girişimlerinden ve yanlış bilgilerden korumak için çok önemlidir. İşte güvende kalmanıza yardımcı olacak bazı yönergeler:

1.Şüpheci olun: İnternette karşılaştığınız bilgilerin kaynağını ve geçerliliğini sorgulayın. Bir şey gerçek olamayacak kadar iyi görünüyorsa veya tam olarak doğru görünmüyorsa, herhangi bir işlem yapmadan önce daha fazla araştırma yapmak en iyisidir.

2. Yazım hatalarını ve şüpheli e-posta adreslerini kontrol edin: Yazım hataları içeren veya yasal olmayan e-posta adresleri kullanan e-postalara, mesajlara veya web sitelerine karşı dikkatli olun. Bunlar kimlik avı girişimlerinin veya dolandırıcılığın işaretleri olabilir.

3. Kaynağı doğrulayın: Herhangi bir bağlantıya tıklamadan veya ekleri indirmeden önce, bilginin kaynağını doğrulayın. Bilginin meşru olduğundan emin olmak için resmi web sitelerini veya saygın kaynakları arayın.

4.Tıklamadan önce düşünün: Bilinmeyen veya şüpheli kaynaklardan gelen e-posta veya mesajlardaki bağlantılara veya eklere tıklamaktan kaçının. Tıklamadan önce gerçek URL'yi görmek için bağlantıların üzerine gelin.

5.Aniden ortaya çıkan mesajlara karşı dikkatli olun: Bir arkadaşınızdan veya tanıdığınızdan karakter dışı veya beklenmedik görünen bir iletişim alırsanız, herhangi bir işlem yapmadan önce kaynağı doğrulayın. Hesapları ele geçirilmiş olabilir.

6.Güvenlik yazılımı kullanın: Cihazlarınıza antivirüs ve anti-malware yazılımları yükleyin ve düzenli olarak güncelleyin. Bu, kötü amaçlı yazılımların tespit edilmesine ve cihazınıza bulaşmasının önlenmesine yardımcı olabilir.

Eleştirel düşünme becerilerini kullanarak ve bu yönergeleri takip ederek kendinizi çevrimiçi tehditlerden ve yanlış bilgilerden koruyabilirsiniz.

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

ÇEVRİMİÇİ ORTAMDA GÜVENDE OLMAK İÇİN TEMEL YETKİNLİKLER

e. Bulunduğunuz web sitesinin güvenli olduğunu doğrulayın:
Bir web sitesinin güvenliğini doğrulamak, özellikle ödeme bilgileri gibi hassas bilgileri girerken kendinizi çevrimiçi tehditlerden korumak için çok önemlidir. İşte bir web sitesinin güvenliğini doğrulamak için bazı adımlar:

1. URL'yi kontrol edin: Web sitesinin URL'sine bakın ve sadece "http://" yerine "https://" ile başladığından emin olun. "s" güvenli anlamına gelir ve web sitesinin tarayıcınız ile web sitesi arasında iletilen verileri şifreleyen bir SSL sertifikasına sahip olduğunu gösterir.

2. Bir asma kilit simgesi arayın: Adres çubuğunda URL'nin yanında bir asma kilit simgesi olup olmadığını kontrol edin. Bu, web sitesinin güvenli olduğunu ve HTTPS şifrelemesi kullandığını gösterir.

3. Web sitesinin yasallığını doğrulayın: Herhangi bir kişisel bilgi veya ödeme bilgisi girmeden önce web sitesinin meşruiyetini doğrulayın. Fiziksel adres ve telefon numarası gibi iletişim bilgilerini arayın ve diğer kullanıcıların yorumlarını veya derecelendirmelerini kontrol edin.

4. Güvenli bir ödeme yöntemi kullanın: Çevrimiçi alışveriş yaparken, PayPal veya kredi kartı gibi alıcı koruması sunan güvenli bir ödeme yöntemi kullanın. Dolandırıcılığa karşı daha az koruma sağladıkları için banka kartı veya banka havalesi kullanmaktan kaçının.

5. Yüksek güvenlikli bir tarayıcı kullanın: Yerleşik kimlik avı ve kötü amaçlı yazılım koruması gibi ek güvenlik özellikleri sunan bir tarayıcı kullanmayı düşünün. Bazı tarayıcılar, bir web sitesinin güvenli olduğunu göstermek için yeşil bir adres çubuğu veya başka göstergeler de görüntüler.

6. Tarayıcınızı ve güvenlik yazılımınızı güncelleyin: En son tehditlere ve güvenlik açıklarına karşı korunmak için tarayıcınızı ve güvenlik yazılımınızı güncel tutun.
Bu yönergeleri izleyerek, ziyaret ettiğiniz web sitelerinin güvenli olmasını sağlamaya yardımcı olabilir ve alışveriş yaparken veya internette gezinirken kendinizi çevrimiçi tehditlerden koruyabilirsiniz.

f.Dijital ayak izinizin farkında olun.
Bir kez çevrimiçi, her zaman çevrimiçi: çevrimiçi olarak yayınlanan her şey, herkesin görmesi için oradadır, sosyal medya profillerinde kullanılan tanımlanabilir bilgilere ve ziyaret edilen, kayıt olunan veya kullanıcının kişisel bilgilerinin herhangi bir türünü tutan sitelere dikkat etmek gerekir.

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

ÇEVRİMİÇİ GÜVENLİK İÇİN PROAKTİF ÖNLEMLER VE YÖNERGELER

Daha güvenli bir yaklaşım benimsemek, bireylerin potansiyel riskleri fark etmelerine ve kendilerini korumak için proaktif önlemler almalarına yardımcı olduğundan, çevrimiçi ortamda güvende kalmak için çok önemlidir. İşte akılda tutulması gereken bazı önemli noktalar:

1.Sahte güvenlik duygusuna karşı dikkatli olun: Bilgisayarlar güvenli görünse de, çeşitli çevrimiçi tehditlere karşı savunmasız olabilirler. Siber suçluların internet üzerinden kimlik hırsızlığı, mali kayıp ve cihazlarınıza zarar verme gibi gerçek zararlara neden olabileceğini unutmamak önemlidir.

2. Bilgi sahibi olun: En son çevrimiçi tehditler ve en iyi güvenlik uygulamaları hakkında kendinizi bilgilendirin. Bu, potansiyel riskleri tanımanıza ve kendinizi korumak için uygun önlemleri almanıza yardımcı olabilir.

3. Güvenlik önlemlerini takip edin: Güçlü, benzersiz parolalar kullanmak, yazılımınızı güncel tutmak ve şüpheli bağlantılara veya eklere tıklamaktan kaçınmak gibi yukarıda tartışılan güvenlik önlemlerini uygulayın.

4.Sağduyunuzu kullanın: Çevrimiçi etkileşimde bulunurken sağduyunuzu kullanın. Bir şey gerçek olamayacak kadar iyi görünüyorsa veya doğru gelmiyorsa, dikkatli davranmak ve bundan kaçınmak en iyisidir.

5. Proaktif olun: Kendinizi çevrimiçi ortamda korumak için verilerinizi düzenli olarak yedeklemek, güvenlik yazılımı kullanmak ve çevrimiçi paylaştığınız bilgiler konusunda dikkatli olmak gibi proaktif adımlar atın.

6. Tetikte olun: Tetikte olun ve çevrimiçi çevrenizin farkında olun. İstenmeyen e-postalara, mesajlara veya kişisel bilgi taleplerine karşı dikkatli olun ve herhangi bir işlem yapmadan önce kaynağı doğrulayın.

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

ÇEVRİMİÇİ GÜVENLİK İÇİN PROAKTİF ÖNLEMLER VE YÖNERGELER

Daha güvenli bir zihniyet benimseyerek ve bu yönergeleri izleyerek, kendinizi çevrimiçi tehditlerden korumaya yardımcı olabilir ve daha güvenli bir çevrimiçi deneyimin keyfini çıkarabilirsiniz.

-Daha güçlü parolalar oluşturun.
Güçlü bir parola, hesaplarınızı ve özel bilgilerinizi bilgisayar korsanlarından korumanın en iyi yollarından biridir.

-Tarayıcı güvenlik özellikleri
Bilgisayarlar Web'de gezinirken virüsler, kötü amaçlı yazılımlar ve casus yazılımlar da dahil olmak üzere farklı tehditlerle karşı karşıya kalır. İyi haber ise web tarayıcınızın bilgisayarınızı korumaya yardımcı olacak birçok yerleşik güvenlik özelliğine sahip olmasıdır.

-Spam ve oltalama yazılımlarını önleme
E-posta dolandırıcılığından, kötü amaçlı yazılımlardan ve kimlik hırsızlığından korunmak için, potansiyel olarak tehlikeli içeriğin nasıl belirleneceğini ve bunlardan nasıl kaçınılacağını anlamak gerekir.

-Bir anti-virüs ile kötü amaçlı yazılımlardan kaçının.
Kötü amaçlı yazılımlar, çevrimiçi olduğunuzda bilgisayarınız için en yaygın tehlikelerden biridir, ancak kaçınılması kolaydır, bilgisayarınızı güvence altına almak ve şüpheli bağlantıları nasıl belirleyeceğinizi ve bunlardan nasıl kaçınacağınızı öğrenmek temel unsurlardır.

-Güvenli online alışveriş
Online alışveriş, evinizin rahatlığında alışveriş yapmanın kolay bir yoludur. Birçok faydası olsa da bazı riskleri de vardır. Finansal verilerinizi korumanın ve güvende olmasını sağlamanın, web sitesinin güvenliğini ve doğruluğunu doğrulamak gibi yolları vardır.

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

EBEVEYN KONTROLLERİ

Ebeveyn kontrolleri, çocuğunuzun çevrimiçi güvenliğini sağlamak için hayati bir araçtır. İşte dikkate alınması gereken bazı önemli noktalar:

1.İçerik filtreleme: Ebeveyn kontrolleri, çocuğunuzun çevrimiçi erişebileceği içeriği filtrelemenize, uygunsuz web sitelerini ve materyalleri engellemenize olanak tanır.

2.Zaman sınırları: Çevrimiçi ortamda çok fazla zaman geçirmediğinden emin olmak için çocuğunuzun çevrimiçi etkinlikleri için zaman sınırları belirleyin.

3.Uygulama ve oyun kontrolleri: Çocuğunuzun hangi uygulamaları ve oyunları indirebileceğini ve bunlara erişebileceğini kontrol ederek yaşına uygun olmalarını sağlayın.

4.Gizlilik ayarları: Çocuğunuzun kişisel bilgilerini korumak için gizlilik ayarlarının doğru yapılandırıldığından emin olun.

5.İzleme ve takip: Bazı ebeveyn kontrol araçları çocuğunuzun çevrimiçi faaliyetlerini izlemenize ve konumlarını takip etmenize olanak tanır.

6.Eğitim ve iletişim: Çocuğunuzu çevrimiçi güvenlik ve sorumlu internet kullanımının önemi hakkında eğitmek önemlidir. Çevrimiçi ortamda karşılaşabilecekleri endişeleri veya sorunları tartışırken kendilerini rahat hissetmeleri için açık iletişimi teşvik edin.

7.Ayarları düzenli olarak gözden geçirin: Çocuğunuzun yaşına ve olgunluk seviyesine uygun olduklarından emin olmak için ebeveyn kontrolü ayarlarınızı düzenli olarak gözden geçirin ve güncelleyin.

Unutmayın, ebeveyn kontrolleri değerli bir araç olsa da kusursuz değildir. Çocuğunuza eleştirel düşünme becerilerini ve dayanıklılığı öğretmek de önemlidir, böylece çevrimiçi dünyada güvenli ve kendinden emin bir şekilde gezinebilir.

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

FARKLI EBEVEYN KONTROLÜ TÜRLERİNİN DAĞILIMI

Ebeveyn denetimleri, ebeveynlerin çocuklarının çevrimiçi etkinliklerini yönetmelerine yardımcı olmak için çeşitli özellikler sunar. İşte farklı ebeveyn denetimi türlerinin bir dökümü:

1.Filtreleme ve engelleme: Bu özellikler, ebeveynlerin uygunsuz olduğunu düşündüğü belirli web sitelerine, kelimelere veya görüntülere erişimi sınırlar. Çocukların çevrimiçi zararlı içeriğe erişmesini önlemeye yardımcı olabilirler.

2. Gönderilen içeriği engelleme: Bu özellik, çocukların kişisel bilgilerini çevrimiçi olarak ve e-posta yoluyla paylaşmalarını önleyerek gizliliklerinin ve güvenliklerinin korunmasına yardımcı olur.

3. Zaman sınırlama: Ebeveynler, çocuklarının ne kadar süre çevrimiçi olmalarına izin verileceği ve günün hangi saatlerinde internete erişebilecekleri konusunda zaman sınırları belirleyebilir. Bu, ekran süresinin yönetilmesine yardımcı olabilir ve çocukların uygunsuz zamanlarda çevrimiçi olmamasını sağlayabilir.

4. İzleme araçları: Bu araçlar, erişimi engellemeden ebeveynleri çocuklarının çevrimiçi faaliyetleri konusunda uyarır. Bir çocuğun hangi web sitelerini ziyaret ettiğini kaydedebilir ve belirli siteleri ziyaret ettiklerinde uyarı mesajları görüntüleyebilirler. Bu, ebeveynlerin çocuklarının çevrimiçi davranışları hakkında bilgi sahibi olmalarını sağlar.

Ebeveyn kontrolleri çocukların çevrimiçi ortamda korunmasına yardımcı olsa da, eğitim, sorumluluk ve yetişkin gözetiminin yerini tutmadığını unutmamak önemlidir. Ebeveynler çocuklarını internetin potansiyel riskleri hakkında eğitmeli ve uygun ve uygunsuz web siteleri hakkında kurallar koymalıdır. Çocuklarla açık ve dürüst konuşmalar, çevrimiçi ortamda karşılaşabilecekleri endişeleri veya sorunları tartışırken kendilerini rahat hissettikleri güvenli bir çevrimiçi ortam yaratmanın anahtarıdır.

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

EBEVEYN GÖZETİMİNE İLİŞKİN TEMEL KILAVUZLAR

Ebeveyn gözetimi, çocukların çevrimiçi güvenliğini sağlamak için çok önemlidir. İşte etkili ebeveyn denetimi için bazı temel kurallar:

1.Birlikte çevrimiçi zaman geçirin: Çocuklara uygun çevrimiçi davranışları onlarla çevrimiçi zaman geçirerek öğretin. Bu, faaliyetlerini izlemenize ve olası riskleri tartışmanıza olanak tanır.

2.Bilgisayarı ortak bir alanda tutun: Bilgisayarı, kullanımını kolayca izleyebileceğiniz oturma odası gibi evin ortak bir alanına yerleştirin. Bilgisayarları bireysel yatak odalarına yerleştirmekten kaçının ve akıllı telefonlarda veya tabletlerde geçirilen zamanı izleyin.

3.Çocukların favori sitelerini yer imlerine ekleyin: Çocukların favori sitelerini kolay erişim için yer imlerine eklemek, internette güvenli bir şekilde gezinmelerine yardımcı olur ve uygunsuz içeriğe erişme riskini azaltır.

4.Finansal hesapları kontrol edin: Finansal hesapları, kart ekstrelerini ve telefon faturalarını, yetkisiz çevrimiçi satın alımlara işaret edebilecek herhangi bir alışılmadık ücret için düzenli olarak kontrol edin.

5.Çevrimiçi koruma hakkında bilgi alın: Çocuğunuzun okulunda, okul sonrası merkezinde, arkadaşlarının evinde veya çocukların gözetimsiz bilgisayar kullanabileceği başka herhangi bir yerde hangi çevrimiçi koruma önlemlerinin uygulandığını öğrenin.

6.Raporları ciddiye alın: Çocuğunuz rahatsız edici bir çevrimiçi alışveriş veya olay bildirirse, bunu ciddiye alın ve sorunu derhal araştırın. Çocuğunuzun sahip olabileceği endişeleri tartışırken rahat hissetmesi için açık iletişimi teşvik edin.

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

EBEVEYN GÖZETİMİNE İLİŞKİN İPUÇLARI

İngiltere Daha Güvenli İnternet Merkezi direktörü Will Gardner, çocuklarının ve ailelerinin internetle ilişkisini yönetmek isteyen ebeveynler veya bakıcılar için bazı yararlı bilgiler sunuyor. Erişim adresi: https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

- Aile üyelerinize (özellikle çocuklarınıza) internetin onları nasıl hissettirdiğini sorun
"Çocuğunuzla teknolojiyi nasıl kullandıkları hakkında düzenli olarak konuşun ve favori siteleri ve hizmetleri de dahil olmak üzere dijital yaşamlarının nasıl olduğunu ve çevrimiçi olmanın onlara nasıl hissettirdiğini öğrenin. Çocuğunuzu dinlemek, onu nasıl destekleyebileceğiniz konusunda size mümkün olan en iyi fikri verecektir."

- Çocukları kısıtlamalarla bunaltmak faydalı değildir
"Ebeveynler olarak çocuğunuzun çevrimiçi olmasının yarattığı riskler konusunda endişe duymanız doğaldır, ancak gençler için çevrimiçi dünya heyecan verici ve eğlencelidir, çünkü onlar için pek çok fırsat sunmaktadır.
"Çocuğunuzun teknolojiyi ve interneti, her şeyin dijital olduğu bir dünyada büyüdüğü için farklı şekillerde kullanacağını unutmayın. Çevrimiçi olmanın hem olumlu hem de olumsuz yönlerine bakmaya çalışın ve çocuğunuzu kısıtlamalarla bunaltmak yerine yapabileceği güvenli seçimlerle güçlendirin."

- Kullandıkları uygulamaları ve hizmetleri tanıyın.
"Sosyal medyadaki gizlilik ayarları gibi özellikleri kullanarak ve bir dizi uygulama, oyun ve hizmet hakkında nasıl raporlama yapılacağını anlayarak çocuğunuzu çevrimiçi ortamda desteklemek için adımlar atabilirsiniz."

- Yardım için mevcut araçları kullanın.
"Aileniz tarafından kullanılan cihazları yönetmenize yardımcı olacak çok sayıda araç bulunmaktadır. Örneğin, ebeveyn kontrollerinin nasıl etkinleştirileceğini ve kullanılacağını bilmek çocuğunuzun internette uygunsuz içerik görmesini engellemeye yardımcı olabilir."

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

İNTERNET GÜVENLİĞİ KONTROL LİSTESİ

Norton Güvenlik Merkezi'ne göre, çevrimiçi ortamda güvenli davranmak, sizin ve ailenizin internette cihazlarınıza, kişisel bilgilerinize veya ailenize zarar verebilecek istenmeyen bilgilere, materyallere veya risklere maruz kalmasını önlemeye yardımcı olabilir. Daha önce bahsettiğimiz bazı yaygın tehlikelerin kurbanı olmamaları için özellikle çocuklara bilgisayar güvenliğini öğretmek akıllıca olacaktır.

İşte Norton Güvenlik Merkezi'nin tavsiyelerine dayanan bir İnternet Güvenliği Kontrol Listesi:

1.Güçlü, benzersiz parolalar kullanın: Yetkisiz erişime karşı korumak için tüm hesapların güçlü, benzersiz parolalara sahip olduğundan emin olun.

2.Yazılımı güncel tutun: Güvenlik açıklarına karşı korunmak için işletim sistemlerini, tarayıcıları ve güvenlik yazılımlarını düzenli olarak güncelleyin.

3.Güvenlik yazılımı kullanın: Virüslere ve diğer tehditlere karşı korunmak için saygın antivirüs ve anti-malware yazılımları yükleyin.

4.Kimlik avı dolandırıcılığına karşı dikkatli olun: Kişisel bilgi isteyen veya şüpheli bağlantılar içeren e-postalara, mesajlara veya web sitelerine karşı dikkatli olun.

5.İki faktörlü kimlik doğrulamayı etkinleştirin: Ekstra bir güvenlik katmanı için bunu sunan hesaplarda iki faktörlü kimlik doğrulamayı etkinleştirin.

6.Güvenli ağlar kullanın: Hassas faaliyetler için halka açık Wi-Fi kullanmaktan kaçının ve gerektiğinde sanal özel ağ (VPN) kullanın.

7.Çocukların çevrimiçi etkinliklerini izleyin: Çocukların çevrimiçi faaliyetlerine göz kulak olun ve onları güvenli internet uygulamaları konusunda eğitin.

8.Önemli verileri yedekleyin: Kötü amaçlı yazılım veya donanım arızası nedeniyle veri kaybına karşı korunmak için önemli verileri düzenli olarak yedekleyin.

9.Kişisel bilgi paylaşımını sınırlayın: Kişisel bilgileri çevrimiçi paylaşma konusunda dikkatli olun ve bunu yalnızca güvenli, saygın web sitelerinde yapın.

10.Kendinizi ve ailenizi eğitin: En son çevrimiçi tehditler hakkında bilgi sahibi olun ve ailenizi güvenli internet uygulamaları konusunda eğitin.

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

KAYNAKÇA

Ailelerin çevrimiçi ortamda daha güvenli kalmalarına yardımcı olacak internet güvenliği ipuçları ve kontrol listesi. Norton Güvenlik Merkezi. Erişim adresi: https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html

Çevrimiçi gizliliğinizi nasıl korursunuz? Norton Güvenlik Merkezi (2021) https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

İnternet Güvenliği: Spam ve Kimlik Avından Kaçınma. GCFGlobal (2021) Erişim adresi: https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/

Ebeveyn kontrolleri. İnternet konuları (2021) https://www.internetmatters.org/parental-controls/

Her ebeveynin bilmesi gereken 5 siber güvenlik ipucu. Norton Güvenlik Merkezi. Erişim adresi: https://us.norton.com/internetsecurity-kids-safety-5-cybersafety-tips-every-parent-should-know.html

Web tehditleri nelerdir? Kaspersky (2021) Erişim adresi: https://thebossmagazine.com/internet-safety-tips/

Dijital ayak izi nedir? netsafe (2021) https://www.netsafe.org.nz/digital-footprint/

Çevrimiçi Güvenlik Nedir? National Online Safety (2021) Erişim adresi: https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety

Kişisel bilgileri sosyal medyada paylaşmanın tehlikeleri.

Patel, D., Mayıs 2020, PennToday. Erişim adresi: https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

STEGNER, Ben. (2017) Ebeveyn kontrolleri için eksiksiz kılavuz. MUO: Teknoloji açıklaması. Erişim adresi: https://www.makeuseof.com/tag/guide-parental-controls/

İnternette güvende kalmak: ebeveynler ve gençler için kılavuz ilkeler

https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

Özel bilgilerinizi çevrimiçi ortamda nasıl koruyabilirsiniz? İngiltere Norton Güvenlik Merkezi https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html

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