CİHANBEYLİ REHBERLİK VE ARAŞTIRMA MERKEZİ

ŞUBAT 2021 E-DERGİ

BİLİNÇLİ İNTERNET KULLANIMI

Bilinçli İnternet Kullanımı Nedir?
Bilinçli İnternet Kullanımı Nasıl Olur?

İnternet Ortamında Karşılaşılabilecek Riskli Durumlar

Bilinçli İnternet Kullanımı İçin Öneriler

İLETİŞİM
964695@meb.k12.tr
03326734126

BİLİNÇLİ İNTERNET KULLANIMI NEDİR?

Çağımızın en güçlü kitle iletişim kaynaklarından biri olan bilgisayar ve yaşamımıza birden bire giren internet, bugün **bilgilenme, işlem yürütme, haberleşme, eğitim ve eğlence** fonksiyonlarıyla hayatımızın ayrılmaz bir parçası olmuştur.

Her yaştan insanın günlük hayatında İnterneti bilinçli ve faydalı bir şekilde kullanmasının pek çok faydası bulunur. Ancak, pek çok uzman, İnternetin bilinçsiz kullanımının, insanlar üzerinde zararlı etkileri olduğunu ve bazı fiziksel, sosyal ve psikolojik sorunlara yol açtığını belirtmektedir.

TEKNOLOJİYİ NASIL KULLANMALI?

Bilinçli teknoloji kullanımı sürecinde İnsanlık için faydalı olan İnternetin zararlarının da iyi bilinmesi ve bu konuda gereken önlemlerin alınması oldukça önemlidir.

Hayatta her şeyin bir sınırı vardır; yemenin, gezmenin, çalışmanın bir sınırı olduğu gibi teknolojinin de bir sınırı olmalıdır.
Ancak doğru ve sınırlı kullanarak teknolojiden faydalanabilirsiniz.
Teknoloji hayatınızı sınırlamasın siz kullanımınızı sınırlayın.

BİLİNÇLİ İNTERNET KULLANIMI NASIL OLUR?

- İnternetin bilinçsiz ve aşırı kullanımı geleceğimizi düşünmemizi, geleceğe yönelik hedefler belirlememizi ve hayal kurmamızı engeller. Bizi bugüne hapseder. Geleceğimizi düşünebilmek için interneti sınırlı kullanmalıyız.

- Ders çalışırken telefonunun çocuğun yanında olması dersine yoğunlaşmanızı zorlaştırabilir. Sürekli bakma ihtiyacı hissedebilir, bildirimler rahatsız edebilir ve bu sebeple akademik performansı düşebilir.

- Çocuk her boş zamanını cep telefonuyla, tablet veya bilgisayarla geçirmemelidir. Boş zamanlarında başka şeyler de yapmalı ki, internet çocuğunuzu esir almasın.

- Teknolojiye ayırmadığınız vakitler de olsun. Çocukların ailesiyle, arkadaşlarıyla ya da kendisiyle baş başa kalıp internet dışında da var olabileceğini hissetmesi önemlidir.

- Çocuklar arkadaşları ile iletişim kurarken sadece sanal ortamları tercih etmemelidir. Yüz yüzeyken oyunların daha heyecanlı, sohbetlerinizin daha neşeli olduğunu görmesi sağlanmalıdır.

Gerçek hayatta dikkat edilmesi gereken gizlilik ve güvenlik kurallarının sanal ortamda da aynen geçerli olduğunu unutmayın. Dışarıda kendinize dikkat ederek birçok önlem aldığınız gibi sanal dünyada da kendinizi korumanız gerektiğini asla unutmayın.

- Kişisel ve ailevi özel bilgiler sanal ortamlarda paylaşılmamalıdır. Unutmayın sanal ortamlara aktarılan bilgiler çok çabuk kopyalanabiliyor.

- Çocuklara sanal arkadaşlıkların tehlikeleri olabileceği anlatılmalıdır. Karşınızdakinin gerçek kimliğini, yaşını ve niyetini bilmeniz sanal ilişkilerde zordur.

- Sanal ilişkilerde kişisel sınırlara dikkat edilmelidir. Çocuklar tanımadığı kişilerden gelen arkadaşlık tekliflerini ve mesajlarını kabul etmemelidir.

Kaynaklar;

- https://orgm.meb.gov.tr/meb_iys_dosyalar/2020_11/13161116_ORTAOKUL_OYGYRENCIY.pdf
- https://www.odtugvo.k12.tr/ankara/pdf/Ergenlerde_Bilincli_Teknoloji_KullanYmY.pdf

İNTERNET ORTAMINDA KARŞILAŞILABİLECEK RİSKLİ DURUMLAR

İnternet insan hayatını kolaylaştırıcılığı ile insanlık tarihinin en önemli buluşlarından biridir. İnternetin hayatı kolaylaştırıcılığınınyanında kullanım konusundaki hatalardan kaynaklı, bireyler için risk oluşturan yönleri bulunmaktadır. İnternet ortamında karşılaşılabilecek riskler olumsuz sonuçlar ortaya çıkarabilmektedir. Özellikle çocukları ve gençleri bu risklerden korumak bir gerekliliktir.

İnternet ortamında karşılaşılabilecek riskli durumlar;

- Yanlış ve zararlı bilgiye erişim:internet ortamında erişilen bilgilerin tamamı doğru ve güvenilir değildir.

- Siber Zorbalık: Siber zorbalık, dijital teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Bu tür zorbalıklar sosyal medyada, mesajlaşma platformlarında, oyun platformlarında ve cep telefonlarında görülebilir.Hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranıştır. Sosyal medyada bir kişi hakkında yalanlar yaymak ya da utandırıcı fotoğraflar yayınlamak, incitici mesajlar ya da tehditler yollamak, başka birinin kimliğiyle başkalarına kötü mesajlar göndermek gibi durumlar siber zorbalıktır.

- Sanal Dolandırıcılık: İnternet ortamındaki bilgilerin kopyalanarak, çalınarak yada sahte siteler ve hesaplar kullanılması yoluyla vb. bireylerin aldatılması, maddi zarar görmesi.

- Kişisel Bilgilerin Paylaşımı ve Kimlik Hırsızlığı (identity theft): kişisel bilgilerin çalınması, kopyalanması yoluyla gizlilik ve kişisel verilerin korunması gibi durumların ihlal edilmesi yoluyla ortaya çıkabilmektedir.

- Zararlı Yazılımlar: programlanabilir herhangi bir aygıta, hizmete veya ağa zarar vermek veya bunlardan yararlanmak üzere tasarlanmış her türlü zararlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için kurbanlardan veri elde ederek baskı yapmak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara ve parolalara kadar değişebilir. Kötüye kullanılabilecek bilgi türü sonsuzdur.

- Oltalama (phishing):Dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür. E-postalar, bilinen web sitelerinden veya kullanıcının bankasından, kredi kartı şirketinden, e-posta veya internet hizmeti sağlayıcısından gönderilmiş gibi gözükür. Genellikle hesapları güncelleyebilmek için kredi kartı numarası veya şifre gibi kişisel bilgiler sorulur. Bu e-postalarda kullanıcıları bir başka web sitesine yönlendiren URL bağlantısı yer alır. Bu site aslında ya sahte ya da değiştirilmiş bir web sitesidir. Kullanıcılardan da bu siteye gittiklerinde phishing saldırısını yapan kişiye iletilmek üzere kişisel bilgilerini girmeleri istenir. Phishing, genelde bir kişinin şifresini veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır.

Bir banka veyar esmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Phishing saldırıları için bankalar, sosyal paylaşım siteleri, e-posta servisleri, online oyunlar vb. sahte web sayfaları hazırlanmaktır.

Burada bilgisayar kullanıcısından kimlik bilgileri, kart numarası, şifresi vb. istenir. E-posta mesajındaki ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

- Uygunsuz içeriklere erişim: Çıplaklık, taciz, şiddet, saldırganlık vb. içeren içerikleri barındırması yönü riskli bir durumdur.

- Yasadışı Kumar: Yasa dışı online şans oyunlarının ve bahis oyunlarının bulunması ve oynanması riskli durumlardır.

- Teknoloji/İnternet Bağımlılığı:Teknolojinin insan hayatına getirdiği sayısız faydalar var. Ancak kişinin teknoloji kullanımı üzerinde kontrolünün kaybolması ve teknolojiyi ölçüsüz ve sınırsız kullanması çok ciddi

zararlara sebep olabilir. İnternet ve teknoloji bağımlılığı diğer bağımlılıklarda olduğu gibi kişinin bağımlısı olduğu teknolojik ürüne ulaşamadığında yoksunluk yaşadığı bir durum olarak tanımlanmaktadır.

- Sağlık Sorunları:İnternetin başında aşırı zaman geçirmeye bağlı olarak görülebilecek fiziki ve psikolojik rahatsızlıklardır.
- Yabancılarla Çevrimiçi ve Çevrimdışı İletişim: sahte kimlikler ve hesaplar, zarar verme amaçlı iletişim kurma durumları olduğundan yabancılarla iletişim tehlikeli sonuçlar ortaya çıkarmaktadır.
- Şiddet/Nefret/Irkçılık Faaliyetleri,Silah ve Madde Kullanımı gibi suç teşkil eden durumlarla ilgili risk taşımaktadır.
- Telif Hakları İhlali: Bilgilerin kaynak gösterilmeksizin kullanılması.

Gorüldüğü üzere internet hayatımıza getirdiği pek çok yenilik yanısıra bir o kadar da riski beraberinde getirmiştir. Bunun için başta dijital vatandaşlık algısının ve dijital okur-yazarlık seviyesinin çocuk yaşlardan başlanarak geliştirilmesi için hem bireysel hem toplumsal bazda atılması gereken adımlar mevcuttur. Tüm bunlar yeni yetişen neslin çok iyi birer dijital kullanıcı olduğunun farkında olarak hareket edilmesi gerekliliğini de doğurmaktadır.

İnternete erişimi konusunda tamamen kısıtlanmasının imkânsız olduğunu farkında olarak; çocuklara ve gençlere dijital teknolojileri etik, bilinçli ve sorumlu birer birey olarak kullanma alışkanlığı kazandırılmalıdır.

KAYNAKLAR
https://internet.btk.gov.tr/internetin-riskleri-ve-zararlari
https://www.unicef.org/turkey/siber-zorbalık-nedir-ve-nasıl-önlenir
https://bim.aku.edu.tr/phishing-oltalama-nedir
https://www.yesilay.org.tr/tr/bagimlilik/teknoloji-bagimliligi

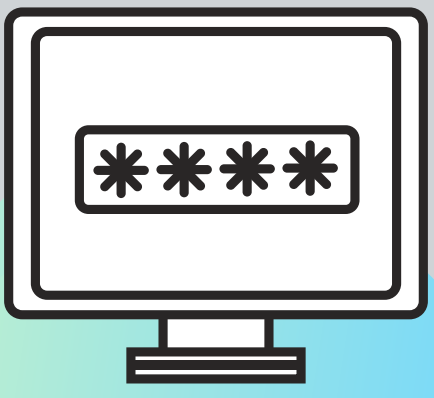
BİLİNÇLİ İNTERNET KULLANIMI İÇİN ÖNERİLER

- Teknolojik cihazlarla çocuklarınızı yalnız bırakmayın. Çocuklar sosyal medya ağları vb. sanal ortamlardaki olası tehlikelerin farkına varması ve kötü niyetli kişilerin tuzaklarına karşı yetişkinlere göre daha savunmasızdırlar. Bu yüzden çocuklar tarafından teknolojik cihazların kullanımında ekranın yetişkinler tarafından görülebileceği yerde olması olası tehlikelerin önüne geçer.

- Evinizdeki internet çocuklar tarafından da kullanılıyorsa, servis sağlayıcınızla görüşüp güvenli internet hizmetinden yararlanabilirsiniz.

- İnternetten edinilen haber ya da diğer bilgilerin geçerliliği için kesinlikle bilginin kaynağını araştırın. Kaynağı olmayan ya da doğrulanmış hesapların paylaştığı bilgiler dışındaki bilgiler doğru olmayabilir. Unutmayın, internet sadece güvenilir bilgi kaynakları tarafından değil aynı zaman da insanlara zarar vermek isteyen kötü niyetli kullanıcılar tarafından da oluşturulmuş olabilir.

- Çevrimiçi hesaplarınız için şifrelerinizi girerken kesinlikle sanal klavye kullanın, böylece kötü niyetli kişilerin fiziki tuşlarla yapılan girişlerinizden elde edilebileceği şifrelerin önüne geçmiş olursunuz.



- Kullandığınız tüm çevrimiçi hesapların şifrelerini farklı karmaşık kombinasyonlar halinde düzenleyin. Şifre oluştururken eklenen rakam, özel karakterler, şifrenizin kötü niyetli kişiler tarafından ele geçirilmesini zorlaştıracaktır.

- Resmi kurumların siteleri haricindeki sitelere kimlik bilgilerinizi vermeyin. Unutmayın kötü niyetli kişiler bunları sizlere karşı dolandırıcılık niyeti ile kullanabilir.

- İnternet kullanımınızı sınırlayın. İnterneti kullanmaya başladığınızda ne kadar kullanacağınızı bilin.

- Kaynağını bilmediğiniz elektronik posta içeriklerindeki bağlantılara tıklamayın.

- İnternette daha güvenli bir ortam oluşturabilmek için gördüğünüz yasadışı içerikleri ihbarweb (http://www.ihbarweb.org.tr/) sitesine mutlaka bildirmelisiniz.

KAYNAKLAR

https://www.guvenliweb.org.tr/blog-detay/internetin-bilincli-ve-guvenli-kullanimi-icin-ebeveynlere-tavsiyeler

https://ailevecalisma.gov.tr/yalova/haberler/cocuklarin-bilincli-internet-kullanimi-konusunda-ailelere-oneriler/