BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

GÜVENLİ İNTERNET MERKEZİ
www.gim.org.tr

DİJİTAL MAHREMİYET

OCAK **2021**
www.gim.org.tr

Hazırlayan

Psikolog **Gülşah AKSAKALLI**

Grafik Tasarım

Özlem AĞIRCAN

2021

www.gim.org.tr

İÇİNDEKİLER

Genel olarak kişisel bilgileri başkalarından koruma, neyin kiminle ne kadar paylaşılacağına kişinin kendi karar vermesi durumudur. Mahremiyet bir haktır.

MAHREMİYET, GİZLİLİK DEMEKTİR.

DİJİTAL MAHREMİYET

Nasıl ki gerçek hayatta kişisel bir özel alan oluşturulabiliyor ve her şey herkesle paylaşılmıyorsa, dijital ortamda da aynı şekilde hareket edilmelidir.

Her türlü bilgiye ulaşmayı sağlayan ve birçok alanda hayatı kolaylaştıran internet ortamında bir tık ile birçok işlem yapılabilmektedir. Herhangi bir konuda merak edilen bilgilere internet üzerinden kolaylıkla ulaşabilmekte, dünyanın öbür ucundaki gelişmeler hakkında bilgiler elde edilebilmektedir.

İnternet kullanımı her geçen gün artmaktadır. İnternet, sunduğu sayısız imkânlar yanında birçok riski de barındırmaktadır. Bu risklerin başında özel hayatın gizliliğinin yani dijital mahremiyetin ihlal edilmesi gelmektedir. Bu sebeple internetteki mahremiyet kavramına gereken önemin verilmesi gerekmektedir.

İnternetteki olası tehditlerden haberdar mıyız?

NE KADAR DİKKAT EDİYORUZ?

Kendimizin ve çocuklarımızın dijital mahremiyetini korumak için neler yapıyoruz?

Bu ve benzer soruların cevabını, dijital mahremiyetin korunmasına yönelik tavsiyeler ve ipuçlarını bu kılavuzu takip ederek bulabilirsiniz.

DİJİTAL MAHREMİYETİN KORUNMASI

İnternetin, sosyal medyanın ve dijital araçların çok yoğun kullanıldığı günümüzde dijital mahremiyet, oldukça önem verilmesi gereken bir kavramdır. Günümüzde teknoloji, internet ve sosyal medya ile iç içe olan kullanıcılar, kişisel bilgilerini korumak, dijital mahremiyetlerini sağlamak için iyi bir dijital okuryazar olmak zorundadır. Özellikle çocukları erken yaşta bilinçlendirilmesi ve mahremiyet bilincinin oluşturulması büyük önem taşımaktadır.

İnternet ve sosyal medya gibi dijital platformlarda geçirilen süre hızla artmaktadır. İnternet kullanıcılarının, bu platformlarda oldukça fazla paylaşım yaptıkları görülmektedir. Sosyal medya platformlarında her türlü bilgi, video, fotoğraf vb. içeriklerin paylaşılabilmesi, dijital mahremiyetin ihlal edilmesi riskini beraberinde getirmektedir.

Bireyler, dijital ortamda başkaları tarafından kabul görmek, beğenilmek amacıyla özel kalması gereken bilgilerini dahi paylaşılabilmektedirler. Bu durum, bireylerin kendi istekleri ile özel bilgilerini ifşa etmelerine sebep olmakta ve mahremiyetlerinin ihlal edilmesi riskini ortaya çıkarmaktadır.

Çevrim içi ortamda kişisel her türlü içeriğin, sonrasını düşünmeden paylaşılması, ilerleyen zamanlarda kaygı ve endişe verici bir duruma dönüşebilir. Bu nedenle yapılan paylaşımlara dikkat etmek gerekmektedir.

DİJİTAL AYAK İZLERİ

Nereye giderseniz gidin dijital ayak izleriniz sizinle: Çevrimiçi ortamda paylaşılan bir içeriği silmek inanılmaz derecede zordur.

Dijital ayak izi; herhangi bir kullanıcının internette yaptığı bütün faaliyetleri kapsayan ve nerdeyse hiç silinmeyecek olan her türlü bilgidir.

Kişiler internette video izlerken, arama motorundan herhangi konuda arama yaparken, alışveriş sitelerinden alışveriş yaparken, sosyal ağlarda, yaptıkları paylaşımlar ve beğeniler ile dijital ayak izleri bırakmaktadır. Dijital ayak izinin kontrolü için bilinçli olmak büyük önem taşımaktadır. O halde, paylaşım yapılmadan şu sorular sorulmalıdır:

İnternet üzerinden hangi bilgilerin paylaşılması güvenli ya da güvensizdir?

Gönderilen veya paylaşılan içerikte bilinmesi istenmeyen herhangi bir bilgi var mı?

İnternet ortamında paylaşılan bilginin silinmeyecek oluşu ileride herhangi bir sıkıntı yaratır mı?

Paylaşılan içerikle ilgili bir problem yaşandığında şikâyet süreçleri biliniyor mu?

İnternet ortamına yüklenen herhangi bir içeriğin, sonrasında silinse dahi çevrimiçi ortamda kalmaya devam edebileceği unutulmamalıdır. Paylaşılan fotoğraflar, videolar, metinler kısaca herhangi bir veri internet ortamında hızlıca yayılabilmekte, paylaşan tarafından silinse dahi çevrimiçi ortamda kalmaya devam edebilmektedir.

Çevrimiçi mahremiyeti korumak ve çocuklara mahremiyet bilincini vermek ebeveynlerin en önemli görevlerinden biridir. Ebeveynlerin çocukları ile ilgili paylaşımlarına da dikkat etmeleri önem taşımaktadır. Ebeveynler paylaşımları iyi niyetle yapsa da paylaşılan fotoğraflar başka kişilerce değiştirilebilir, hatta uygun olmayan sitelerde dahi paylaşılabilir.

Bu sebeple;

“PAYLAŞMADAN ÖNCE DÜŞÜN”

yaklaşımından uzaklaşmamak gerekmektedir.

DİJİTAL MAHREMİYETİ KORUMAYA YÖNELİK TAVSİYELER

Dijital mahremiyeti korumak için öncelikle yapılması gereken **dijital güvenliğin** sağlanmasıdır.

Çocuklara güvenilir bilgi vermek, internette güvende kalabilmelerini sağlamak için önce dijital ortamlara yönelik etik kuralları öğretmek, kullanım becerilerinin geliştirilmesini sağlayarak iyi bir dijital okuryazar olmalarına sağlamak gerekmektedir. Bu sayede çocuklar ve gençler, teknolojinin ve internetin zararlarına, kötüye kullanımlarına karşı eğitilebilir ve bu ortamlarda mahremiyetlerini korumalarına katkı sunulabilir.

Dijital Güvenliğimiz İçin Dikkat Edilmesi Gerekenler

- **Oluşturulan parolanın güvenli olmasına dikkat edilmelidir!**

Dijital çağda parolalar büyük önem taşımakta ve güvenliğin temelini oluşturmaktadır. Parolalar, bir evin giriş kapısı gibidir. Kapı güçlü değilse, eve giriş o kadar kolay olur.

Oluşturulan parolanın her yerde kullanılan parola olmamasına dikkat edilmelidir. Eğer herhangi bir hesaba ait parola çalınır, hesap başkasının eline geçerse diğer hesaplara da aynı parola ile erişilebilir.

Parola seçiminde; küçük büyük harf, sembol ve sayılar kullanılmalıdır. Parola ne kadar uzun olursa tahmin etmesi de bir o kadar zor olur. Güvenlik güçlü bir parola ile başlar.

- **Kişisel bilgilerin paylaşılmamasına özen gösterilmelidir!**

Kişisel bilgiler (doğum tarihi, T.C. Kimlik numarası vb.) internet ortamında güvenilirliğinden emin olunmayan yerlerde ve kişilerle paylaşılmamalıdır.

- **Şüpheli linkler tıklanmamalıdır!**

Kaynağından emin olunmayan linkler tıklanmamalı, güvenilmeyen herhangi bir dosya indirilmemelidir. Tıklanan link veya indirilmeye çalışılan dosya virüs içerebilir ve bilgilere zarar vermeye veya kişisel bilgilerin çalınmasına yönelik hazırlanmış olabilir.

- **Güvenilir Kablosuz Ağ (WiFi) kaynakları tercih edilmelidir!**

Herkese açık ve güvenilir olmayan wi-fı kaynakları kullanıldığı takdirde tehditlere açık duruma gelinebilir. Güvenilirliğinden emin olunmayan ağlar kullanılmamalı, kullanımı zorunlu ise VPN kullanımı veya güvenli bağlantı uygulamaları ile güvenirliği sağlanmalıdır. Kötü niyetli kişiler bu tür ağlara bağlanan kişilerin bilgilerini ele geçirebilmekte ve kişileri kolayca mağdur edebilmektedir.

- **E-posta kullanırken istenmeyen ileti (spam) filtrelerine dikkat edilmelidir!**

İstenmeyen e-postalar “spam” filtresi ile engellenebilmektedir. Spam filtresi, istenmeyen ve zararlı olabilecek içerikleri gelen kutusundan kaldırmaktadır. E-postayı güvenli bir şekilde kullanmak için spam özelliğinin aktif hale getirildiğinden emin olunmalıdır.

AKILLI CİHAZLARDA GÜVENLİK VE MAHREMİYET

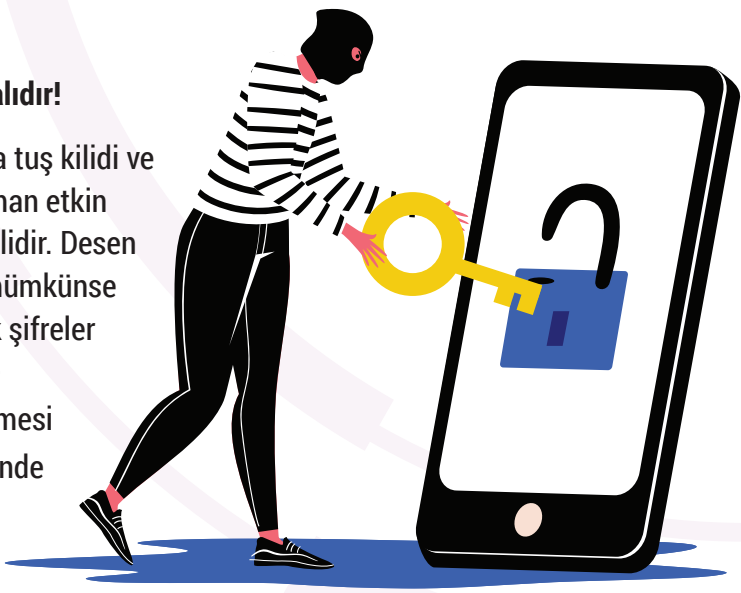
Akıllı cihazlar sosyal ağlar, çevrimiçi alışveriş, internette gezinme vb. birçok etkinlik için kullanılmaktadır. Akıllı cihazları kullanırken de birçok uygulamaya ihtiyaç duyulmaktadır ve bu uygulamaların çoğu kişisel bilgileri kullanmaktadır. Bu sebeple kişisel bilgileri korumak amacıyla bir takım önlemler almak gerekmektedir.

Güvenliği sağlamak için öncelikli olarak;

- **Akıllı cihazlarda**

  ekran kilidi kullanılmalıdır!

Akıllı cihazlar için mutlaka tuş kilidi ve parola belirlemeli, her zaman etkin olmasına özen gösterilmelidir. Desen veya kısa şifreler yerine mümkünse parmak izi gibi biyometrik şifreler tercih edilmelidir. Böylece herhangi birinin eline geçmesi halinde bilgiler daha güvende tutulabilir.



- **Yüklenen uygulamalara dikkat edilmelidir!**

Akıllı cihazların uygulama marketlerinden çeşitli yazılımlar indirilebilmektedir. İndirilen uygulamaların güvenilirliği kontrol edilmeli, uygulamaya ait açıklamalar, yorumlar, indirilme sayıları ve uygulamanın geliştiricisi incelenmelidir. Bunlara ek olarak;

- Uygulamalar Google Play ve App Store gibi resmi uygulama marketlerinden temin edilmelidir. Market dışından indirilen uygulamalar fark edilmeyecek riskleri barındırabilmektedir. (Örneğin, kişisel bilgiler sızdırılabilir, sistem yavaşlatılabilir)
- "Editörün" seçimi, PEGI gibi derecelendirme işaretleri, uygulama puanı ve kullanıcı yorumları yol gösterici olabilir.
- Uygulamanın gereğinden fazla izin isteyip istemediğine dikkat edilmelidir.
- Kullanılmayan uygulamalar kaldırılmalıdır.
- Uygulamalar düzenli olarak güncellenmelidir.

- **Cihazlardaki uygulamalarda nelere izin verildiğine dikkat edilmelidir!**

Uygulamalardan gelen izin taleplerine karşı dikkatli olunmalıdır. Bazı uygulamalar; kamera, mikrofon, fotoğraflar hatta rehbere dahi erişmek istemektedir. Peki, yüklenen uygulamanın gerçekten de rehbere erişmesi gerekli midir?

Bu sebeple akıllı cihazlara uygulama yüklerken izin talepleri konusunda titiz davranılmalıdır.

- **Kullanılmayan cihaz bağlantıları kapalı tutulmalıdır!**

Bluetooth, konum, Wi-Fi ve NFC gibi cihaz bağlantıları kullanılmadığı durumlarda kapalı halde tutulmalıdır. Kullanılmayan bağlantıların kapalı olması siber saldırılara karşı koruma sağlar. Böylece, fotoğraflar, dosyalar vb. kişisel bilgilerin kötü niyetli kişiler tarafından erişebilmesinin önüne geçilebilir.

- **Yazılım güncellemeleri yapılmalıdır!**

Güncel olmayan yazılım ve uygulamalar zafiyet barındırabilir. Bu sebeple sistem yazılımı ve uygulamalar güncel tutulmalıdır.

- **Antivirüs uygulaması kullanılmalıdır!**

İndirilen dosyalar ve akıllı cihazlara yüklenen uygulamalar kötü amaçlı kodlar içeriyor olabilir. Bu kod bir kez başlatıldığında verilerin ele geçirilmesine sebep olabilir ve gizliliğe zarar verebilir. Bunu önlemek için lisanslı iyi bir antivirüs uygulaması yüklemek olası riskleri azaltacaktır. Bazı uygulamalar, mobil cihaz kaybedildiğinde bulmaya, uzaktan verileri silmeye, tehdit olabilecek bilinmeyen arayanları engellemeye ve hangi uygulamaların güvenli olmadığını söyleme gibi daha fazla işlevlere sahiptir.

- **Cihazdaki veriler şifrelenmelidir!**

Çoğu akıllı cihaz yerleşik bir şifreleme özelliğine sahiptir. Şifreleme, verileri okunamaz hale getirme işlemidir. Bu özelliği akıllı cihazlarda bulmak ve verileri şifrelemek için bir şifre girmek yeterlidir.

- **İnternetteki zararlı içeriklerden korunmak için;**

'Güvenli İnternet Hizmeti' kullanılabilir. Güvenli İnternet Hizmeti, internet servis sağlayıcıları tarafından ücretsiz olarak sunulan ve kişileri internetteki zararlı içeriklerden büyük oranda koruyan alternatif bir internet erişimidir. Bilgi almak için "www.guvenlinet.org.tr" sitesi ziyaret edilebilir.

SOSYAL AĞLARDA MAHREMİYET

Sosyal medya araçları toplum, kültür, yaş, cinsiyet ayırt etmeksizin herkesin ortak bir mecrada buluşabildiği alanlardır. Günümüzde sosyal ağ platformları çok yoğun bir şekilde kullanılmaktadır. Bu yoğun kullanım bir takım riskleri ve tehlikeli durumları da beraberinde getirmektedir.

Bazı sosyal medya araçları kişilerin bilgi, ilgi alanlarını paylaşma ve iletişim kurmalarına yönelik kullanılırken bazıları ise sadece eğlence amaçlı kullanılmaktadır. Fotoğraf, video, yer ve konum bilgisi gibi her türden kişisel verinin paylaşıldığı sosyal ağ mecralarını bilinçli ve güvenli bir şekilde kullanmak gerekmektedir.

Sosyal ağlarda hızlı bir şekilde yayılmaya devam eden, sayısız güvenlik açığı içeren 3. parti uygulamaların kullanılmasına izin verilmesi kişisel bilgilerin kötü niyetli kişilerin eline geçmesine neden olabilmektedir. Henüz küçük yaşta olan sosyal medya kullanıcıları da düşünüldüğünde sosyal ağları kullanım yaşlarını bilmek ve önlem almak da büyük önem taşımaktadır.

Sosyal Ağların Kullanım Yaşları

+18 (13-18 yaş arası ebeveyn	+13	+13	+13	+13	+13

SOSYAL AĞLARDA MAHREMİYETİ KORUMAYA YÖNELİK ALINABİLECEK TEDBİRLER

Ebeveynlerin sosyal medya araçlarından gelebilecek olası tehditlere karşı müdahale edebilmeleri için kendilerini geliştirmeleri ve çocuklarını bu doğrultuda yönlendirebilmeleri çok önemlidir.

Sıklıkla kullanılan sosyal medya platformları; **Facebook, Whatsapp, Youtube, Instagram, Twitter, Snapchat** ve son zamanlarda kullanımı daha da artan **TikTok** bunların başında gelmektedir.

Sosyal medya platformlarında hesap oluştururken isim, soyisim, e-posta, telefon numarası, fotoğraf, konum gibi bilgiler toplanmaktadır. Bu sebeple dijital mahremiyeti korumak adına bu platformları kullanırken verilecek her türlü bilgiye dikkat etmek gerekmektedir.

Sosyal ağları kullanırken başlıca dikkat edilmesi gerekenler:

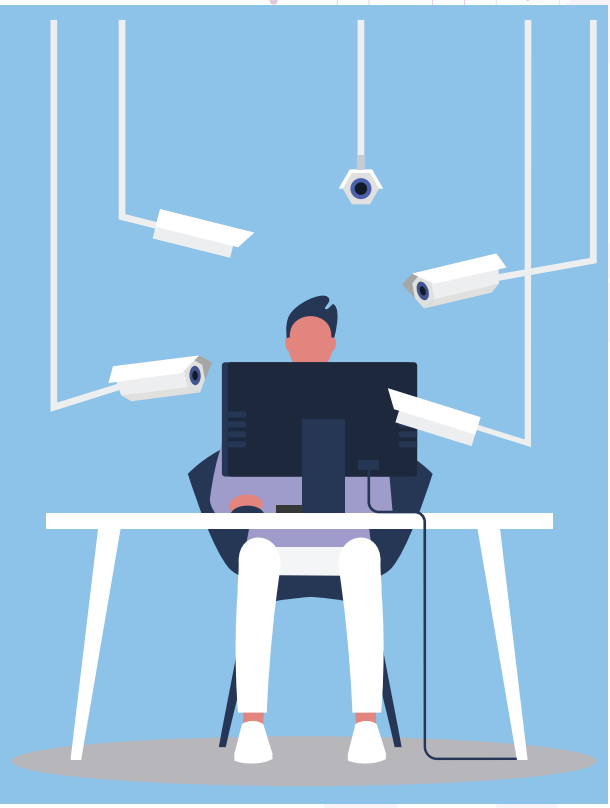
- Kullanılan her sosyal medya platformu için, gizlilik ayarları ile profilin ve paylaşımların kimler tarafından görüleceği mutlaka ayarlanmalı,
- Kötü niyetli paylaşımlar sosyal medya hesabının ilgili şikâyet bölümünden bildirilmeli,
- Mahremiyet kavramı ve çocukların neyi kiminle paylaşabilecekleri ebeveynler tarafından çocuklara etraflıca anlatılmalıdır.
- Tanınmayan kişilerden gelebilecek olan mesajlara dikkat edilmeli, uygunsuz bir içerik

barındırıyorsa sosyal medya hesabının ilgili şikâyet bölümünden bildirilmelidir.

- Tanıdık kişilerin dışında gelen bağlantılar veya güvenilmeyen internet bağlantıları tıklanmamalıdır.
- Ebeveynler çocukların merak ettikleri konuları birlikte araştırmalıdır.
- Çocuklar yaşlarına uygun olmayan herhangi bir konuda video aratıyorsa, onları yargılamadan, meraklarını doğru bilgiyle gidermenin yolları ebeveyn ile birlikte bulunmalıdır.
- Çocukların sosyal medya platformları aracılığıyla kimlerle iletişim kurdukları ve kimleri takip ettikleri ebeveynler tarafından denetlenmelidir.
- Sosyal ağlarda kullanılan 3. parti uygulamaların güvenlik, erişilebilirlik ve gizlilik politikaları sürekli gözden geçirilerek verilen izinler sorgulanmalıdır.

Herhangi bir sosyal medya platformunda sakıncalı görülen içeriklerle karşılaşıldığında mutlaka ilgili platform için şikâyet süreçleri takip edilmeli, gerektiği takdirde ise yasal yöntemlere başvurulmalıdır.

SOSYAL AĞLARDA HAK VE SORUMLULUKLAR



Kişiler, sosyal ağlar da dâhil olmak üzere dijital ortamda bilgiye erişebilme, içerik oluşturma, oluşturulan içerikleri paylaşabilme gibi eşit haklara sahiptir. Başkalarının hak ve özgürlükleri ihlal edilmediği müddetçe herkes düşüncesini özgürce ifade edip paylaşabilir. Özgürce paylaşım yapabilme ve düşünceyi ifade etme hakkı, bir başkasına karşı küfür, şiddet, nefret veya suça teşvik edici içerikleri barındırmamalı ve başkalarının haklarını ihlal edebilecek boyutta olmamalıdır.

Sosyal medya platformları başta olmak üzere dijital ortamın farklı mecralarında kişilik haklarının ihlal edildiği paylaşımlara ve özel hayatın gizliliği ile ilgili sıkıntılara sıklıkla rastlanmaktadır. Yaşanan sıkıntı ve mağduriyetler gerekli tedbirlerin alınmasının zorunluluğunu açıkça ortaya koymaktadır.

Sosyal ağlarda küfür, şiddet, müstehcen vb. içeriklerin yer aldığı paylaşımlar ilgili sosyal medya platformunun şikâyet süreçleri takip edilerek bildirilebilmektedir.

Sosyal ağlarda bulunan güvenlik özellikleri ve şikâyet süreçleri hakkında daha fazla bilgi edinmek için;

*https://www.guvenliweb.org.tr/*sosyal-medya-rehberi ve

*https://internetyardim.org.tr/*icerik-sikayet-surecleri adresleri ziyaret edilebilir.

Ayrıca, sosyal ağlar veya diğer dijital mecralar üzerinden bazen sahte kimlikler oluşturularak bazen ise gerçek kimlik kullanılarak hedef alınan kişiye yönelik yalan haber, hakaret, itibar suikastı gibi içerikler üretilebilmekte ve hızla yayılabilmektedir. Bu sebeple, kişilerin haklarını aramaları noktasında herhangi bir mağduriyet yaşamaksızın hak ve sorumluluklarını bilmeleri büyük önem taşımaktadır.

Kişilik haklarının ihlal edilmesi durumunda yapılabilecekler:

- Medeni kanunun 49'uncu maddesine göre manevi tazminat davası açılabilir.
- 5651 sayılı 'İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9'uncu maddesine göre, ihlalin yapıldığı sitedeki içeriğin çıkartılmasını isteme veya bu isteğin gerçekleştirilmemesi durumunda hakkın ihlal edildiği internet adresine erişimin engellemesi talep edilebilir.
- Kişilik hakları ihlal edilen gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına ya da sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesi talep edebilir.
- İnternet ortamında Kişilik Haklarının İhlali hususunda başvuru yapmak isteyen kişiler, başvuru örneklerine *https://internet.btk.gov.tr* adresinden ulaşabilirler.

Kişilerin haberi olmaksızın özel veya uygun olmayan fotoğraflarının çekilerek internet ortamında paylaşılması, kişilerin mahremiyetlerini tehlikeye düşürmekte ve özel hayatın gizliliğinin ihlal edilmesine sebep olmaktadır. Kanun kapsamında hangi haklara sahip olunduğu ve neler yapılabileceğini bilmek önem taşımaktadır.

Özel hayatın gizliliğinin ihlal edilmesi durumunda yapılabilecekler:

- 5651 sayılı kanunun 9/A maddesine göre; internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiği durumlarda, Bilgi Teknolojileri ve İletişim Kurumu (BTK)'na doğrudan başvurularak içeriğe erişimin engellenmesi talep edilebilir.
- Başvuru için BTK'ya ait *https://www.ihbarweb.org.tr/ohg/* adresi kullanılabilir.

- Hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilmelidir. Bilgilerde eksiklik olması durumunda talep işleme konulmayacaktır.
- BTK' ya gelen talep uygulanmak üzere Erişim Sağlayıcıları Birliği'ne bildirilir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.
- Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi ile yapılır.
- Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan BTK'ya gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar."
- İnternet ortamında özel hayatın gizliliğinin ihlali durumunda başvuru örneklerine ise https://internet.btk.gov.tr adresinden erişilebilmektedir.

Ayrıca, sosyal medya yasası kapsamında gerçekleştirilen düzenleme ile birlikte sosyal ağ sağlayıcılara, kişilik hakkının ve özel hayatın gizliliğinin ihlali durumunda, ilgili kişiler tarafından yapılacak başvuruların cevaplandırılması için en geç 48 saatlik süre içinde olumlu ya da olumsuz cevap verme yükümlülüğü getirilmiştir.

SOSYAL AĞLARDA İÇERİK PAYLAŞ/MA

Dijital dünyada yapılan her paylaşım, paylaşım yapan kişiyi temsil etmektedir. Bu sebeple, internet ortamında herhangi bir içerik paylaşılmadan önce düşünülüp sonra paylaşılmalıdır.

Herkes tarafından görülmesi istenmeyen veya özel olan fotoğraflar paylaşılmamalı, neyin kiminle paylaşıldığına dikkat edilmelidir.

Sosyal ağlarda diğer kullanıcılar ile ilgili fotoğraf veya herhangi bir içeriğin paylaşılması bu kullanıcıların mahremiyetlerini ihlal edebilmektedir. Bu sebeple;

- Yapılan paylaşımlar başka bir kişiye ait fotoğraf veya bilgiyi içeriyorsa mutlaka o kişiden izin alınmalı, aksi takdirde paylaşılmamalıdır.
- Sosyal ağlarda yapılan paylaşımları yabancı kişilerin de görebileceği düşünülerek paylaşımlarda hassas olunmalıdır.

Dijital ortamda paylaşılan bir fotoğraf başka kişiler tarafından yayılabilir bu durum kişisel mahremiyeti tehlikeye sokabilir.

İnternet üzerinden herhangi bir paylaşım yaparken akla hemen şu soru getirilmelidir;

- Paylaştığım fotoğrafı tanımadığım insanlar dâhil herkesin görebileceği bir yere asar mıydım?

Eğer verilen cevap “hayır” ise internet üzerinde herkesin ulaşabileceği bir şekilde fotoğraf paylaşmak iyi bir fikir olmayabilir.

Bu durum paylaşılan her şey için geçerlidir.

SHARENTING

Ebeveynlerin çocuklarının doğumlarından itibaren başlayarak büyüme süreçlerini adım adım sosyal medya üzerinden paylaşmaları çocukların mahremiyet ve gizlilik haklarını da etkilemektedir.

Ebeveynlerin hızla artan fotoğraf paylaşma eylemleri "Sharenting" kavramı ile ifade edilmektedir. Sharenting, İngilizce'de paylaşmak anlamına gelen "share" ve ebeveynlik anlamına gelen "parenting" sözcüklerinden oluşmaktadır.

Masumca ve iyi niyetle paylaşılan bu fotoğraflar çocuk istismarcıları tarafından kötü niyetle kullanılabilmektedir.

İnternet ortamında kötü niyetli kişilerin ve çocuk istismarcılarının olabileceği unutulmamalı, çocukların mahremiyetlerini tehlikeye atacak paylaşımlardan kaçınılmalıdır.

SHARENTING RİSKLERİ VE DİKKAT EDİLMESİ GEREKENLER

Ebeveynlerin diğer ebeveynlerden destek alma, onaylanma veya beğenilme istekleri çocukları ile ilgili daha fazla paylaşım yapabilmelerine neden olabilmektedir. Paylaşılan fotoğrafların veya kişisel bilgilerin kimler tarafından, ne zaman ve nasıl kullanılacağı ise dikkate alınmamaktadır.

DİKKAT !

- Herkese açık bir şekilde paylaşılan çocuk fotoğrafları çocuk istismarcıları tarafından web sitelerinde kötü niyetle kullanılabilir.
- Paylaşılan fotoğraflar çocukların mahremiyetlerini olumsuz etkileyebilir.
- Bebeklikten itibaren sosyal medya aracılığı ile bütün fotoğrafları paylaşılan çocuklar ileriki yaşlarda bu durumdan rahatsızlık duyabilirler.
- Çocukların gizlilik ve mahremiyet konularına karşı bakış açıları farklılaşabilir.
- Dijital kimliğin ön planda tutulması çocuğun gerçek hayatta sorunlar yaşamasına neden olabilir.

Bu nedenle;

Ebeveynlerin çocuklarının sanal dünyadaki mahremiyetlerini gözetmeleri ve onların her anlamda güvenliklerini sağlamaları gerekmektedir.

Ebeveynlerin Çocuklarıyla İlgili Paylaşım Yapmadan Önce Dikkat Etmeleri Gereken 5 Madde:

1. Paylaşılan içerik mahremiyeti ihlal etmemelidir!

Ebeveynler çocukları ile ilgili paylaşım yapmadan önce dijital ortama yüklenen içeriğin gelecekte çocuğa ne hissettirebileceğini mutlaka hesaba katmalıdır. Ebeveynler için masum görünen bir içerik çocuklar için utanç verici olabilir. Çocukların utanabilecekleri bir fotoğrafı dijital ortamda paylaşmak hem mahremiyetlerini riske atacak hem de rahatsız olmalarına neden olacaktır.

2. Bazı içerikler özel kalmalıdır!

Ebeveynlerden bazıları kendilerine veya çocuklarına ait içerikleri ayırt etmeksizin paylaşmaktan hoşlanabilmektedir. Fakat ileride çocuklar ebeveynleri ile aynı görüşte olmayabilir ve bazı içeriklerin kendilerine özel kalmasını tercih edebilirler.

3. Kötüye kullanıma yol açabilecek içerikler paylaşılmamalıdır!

Paylaşılan içeriklerin kimler tarafından görülebileceği mutlaka belirlenmeli, çocukların kişisel bilgilerinin yer aldığı fotoğraflar

paylaşılmamaya özen gösterilmelidir. Çocuklarla ilgili paylaşılan bilgilerin kötü niyetli kişiler tarafından istismar amaçlı kullanılabileceği unutulmamalıdır.

4. Özel hayatın gizliliği ihlal edilmemelidir!

Ebeveynlerinin sürekli olarak sosyal medyada kendileri ile ilgili paylaşım yaptıklarını gözlemleyen çocuklar özel hayatın gizliliği ve mahremiyet kavramlarını farklı algılayabilmektedir. Bu durum mahremiyetin, önemini göz ardı etmelerine sebep olabilmektedir. Mahremiyet bilincinin kazandırılması için önce ebeveynlerin çocuklarına rol model olmaları gerekmektedir.

5. Dijital ortamda çocuklara ait bırakılan izlerin gelecekte karşılarına sorun olarak çıkmasına izin verilmemelidir!

Çocuk hakkında paylaşılan içeriğin herhangi bir zaman diliminde başkaları tarafından görülmesinin sıkıntı yaratabileceği düşünülüyorsa kesinlikle paylaşılmamalıdır. Üniversiteye kabul veya iş başvurularında insanlar hakkında her türlü bilgiye internet ortamından erişilmektedir. Paylaşılan herhangi bir içerik çocuklar için ileride olumsuz bir geri dönüşle sonuçlanabilir.

DİJİTAL OYUNLARDA MAHREMİYET

Günümüzde her geçen gün çocuklar tarafından dijital oyunlara karşı artan bir ilgi görülmektedir. Dijital oyunlar, eğitici-öğretici olmalarının yanında şiddet ve korku gibi unsurları da içerebilmektedir. Şiddet, korku, müstehcenlik vb. olumsuz içeriklere sahip oyunlar çocuklar ve gençler üzerinde birtakım zararlı etkilere de neden olabilmektedir. Ebeveynlerin çocuklarının oynadıkları dijital oyunların hangi türde oyunlar olduğunu bilmeleri ve çocuklarına uygun olup olmadığını kontrol etmeleri büyük önem taşımaktadır.

- **Oyunların Yaş Derecelendirmelerine Dikkat Edilmelidir!**

Yaş derecelendirmeleri, çocukların gelişim düzeyleri için hangi oyunların uygun olduğu konusunda bilgi vermektedir.

2003 yılında ailelerin çocuklarına dijital oyunlar satın alırken daha bilinçli hareket etmelerini hedefleyen bir oyun derecelendirme sistemi olan **PEGI (Pan-European Game Information - Avrupa Oyun Bilgi Sistemi -** www.pegi.info) kurulmuştur. Çeşitli platformlardaki oyun uygulamalarının altında **"PEGI3"- "PEGI7"** benzeri etiketler yer almaktadır. Bu etiketler, PEGI tarafından yapılan değerlendirmeler sonucu oluşturulmuş, oyunların hangi yaş grubu için uygun olduğunu gösteren etiketlerdir.

Ayrıca, Common Sense Media - www.commonsensemedia.org, Entertainment Software Association - www.esrb.org sitelerinden de dijital oyunların yaşa uygunluğu kontrol edilebilmektedir.

- **Oyunlardaki Sohbet Özelliklerine Karşı Dikkatli Olunmalıdır!**

Bazı dijital oyunlar çevrimiçi sohbet özelliği barındırmaktadır. Çocukların tanımadığı kişilerle oyun platformları aracılığıyla bağlantı kurmaları ve psikolojilerini olumsuz etkileyebilecek bir konuşma ile karşılaşmaları durumu onlar için riskli olabilmektedir. Karşılaşılabilecek riskler arasında siber zorbalık, dolandırıcılık, müstehcen içerikli konuşmalara maruz kalma gibi durumlar yer almaktadır.

Ebeveynler olarak, çocukların oynadıkları oyunların özellikleri konusunda bilgi sahibi olunur ve kimlerle iletişim kurduğu bilinirse çocukların güvende olup olmadığı daha kolay saptanabilir.

- **Oyun Akışı ve Reklam İçerikleri Kontrol Edilmelidir!**

Oynanan dijital oyunlar başlangıçta zararsız gibi görünse de ilerleyen bölümlerde olumsuz içerikler barındırabilmektedir. Oyuncuların karşısına küfür, şiddet, müstehcenlik gibi içerikleri barındıran reklamlar çıkabilmektedir.

Bu tarz durumların önüne geçebilmek için ebeveynlerin oyun esnasında çocuklara eşlik etmeleri ve çocukları yönlendirmeleri gerekmektedir.

- **Oyun İçi Satın Almalar Konusunda Dikkat Edilmelidir!**

Bazı oyunlarda yer alan uygulama içi satın alımlar çocuklar için cazip hale gelmekte ve oyunda yükselmek

adına çocukların bilinçsiz bir şekilde oyuna para yatırmalarına sebep olabilmektedir. Uygulama içi satın alımların bilinçsizce ve aşırılığı söz konusu olduğunda bu durum ebeveynleri zor duruma düşürebilmektedir. Bu durumun önüne geçebilmek adına kredi kartı bilgilerinin dijital ortamda kayıtlı olmamasına dikkat etmek gerekmektedir.

- **Oynanan Oyunlarda Kişisel Bilgiler Paylaşılmamalıdır!**

Çevrimiçi oyunlardaki kötü niyetli kişiler, oyuncuların kişisel bilgilerini çalmaya yönelik yöntemler kullanabilmektedir. Kötü niyetli kişiler, elde ettikleri bilgiler ile oyuncuların farklı hesaplarına da erişim sağlayabilmekte veya bu bilgileri siber zorbalık aracı olarak kullanabilmektedir. **Bu sebeple;**

- Oynanan oyunlar için bir takma ad belirlenmeli,
- Gerçek e-posta adresi veya kişisel bilgiler paylaşılmamalı,
- Her bir oyun girişi için ayrı kullanıcı adı ve şifreleri belirlenmeli,
- Çocukların oyun esnasında karşılaştıkları herhangi bir sıkıntılı durum karşısında ebeveynlerine söylemeleri yönünde desteklenmelidir.

DİJİTAL MAHREMİYET VE SİBER ZORBALIK

Çevrimiçi olarak paylaşılan içerikler kimi zaman zararsız gibi görünse de bazen başkaları için sorun yaratabilmektedir. Bu sorunların başında siber zorbalık gelmektedir.

Siber zorbalık; başka bir kişiyi taciz ya da tehdit etmek, utandırmak veya hedef almak için teknolojik araçların kullanılmasıdır.

İnternet üzerinden başkaları ile nasıl bağlantı kurulduğu, nasıl bir konuşma tarzı seçildiği siber zorbalık kavramını anlamak için önemlidir.

Ebeveynlerin çocukların sanal dünyalarına dâhil olmaları olası tehlikelerden ve siber zorbalıktan onları koruyabilmek için önemlidir.

SİBER ZORBALIKLA MÜCADELE İÇİN YAPILABİLECEKLER

Siber zorbalıkla mücadele ederken yasaklayıcı önlemler yerine bilinçli kullanıma teşvik etmek önemlidir. **Bu doğrultuda;**

- İnternet kullanırken dikkat edilmesi gereken davranışların neler olduğu ve nedenleri mutlaka çocuklara açıklanmalıdır.
- Çocukların kendilerine veya başkalarına zarar verebilecek paylaşımlardan kaçınmaları sağlanmalı, pozitif paylaşımlar için yönlendirilmelidir.
- Çocukların paylaştıkları içeriklerin kimler tarafından görülebileceği belirlenmeli, olası riskleri hakkında konuşulmalıdır.
- Çocuklar tanınmayan kişilerden gelen arkadaşlık tekliflerini kabul etmemeleri konusunda uyarılmalıdır.
- Başkası hakkında herhangi bir içerik paylaşmadan önce o kişinin iznini almaları gerektiği öğretilmelidir.
- Herkesin kolaylıkla ulaşabileceği ortamlarda kişisel bilgiler ve özel fotoğraflarını paylaşmadıklarından emin olunmalıdır.
- Siber zorbalığa maruz kalmaları durumunda bunu paylaşmalarının çok önemli olduğu anlatılmalıdır.
- Teknoloji kullanımında evde uygulanan kuralların okulda da hassasiyetle uygulandığından emin olunmalıdır. Gerektiği yerde okul yönetimi ile iletişime geçilmelidir.

DİJİTAL MAHREMİYETİN KORUNMASINA YÖNELİK TAVSİYELER

- Çocukların çevrimiçi ortamda ne kadar zaman geçirecekleri belirlenmeli ve sınırlandırılmalıdır.
- Dijital ortamda çocuklarla birlikte konuşmaya ve öğrenmeye devam edilmelidir.
- Çocuklarla teknoloji hakkında konuşulmalı onlara dijital ortam hakkında neler bildiklerini sorulmalıdır.
- Çocukların sosyal medyada kişisel bilgilerini (yaş, okul, adres, telefon numarası, konum bilgisi) neden paylaşmamaları gerektiği uygun bir dille anlatılmalıdır.
- Açık ve güvenilir bir şekilde iletişim kurulmalıdır. Çocukların iyi veya kötü şeyler hakkında ebeveynleri ile konuşabileceklerini bilmeleri ve rahat hissetmeleri önemlidir.
- Çocukların ziyaret ettikleri web siteleri ve kullandıkları diğer sosyal medya platformları takip edilmeli ve kontrolü sağlanmalıdır.
- Çocukların sosyal medya platformlarının gizlilik ayarlarını bildiğinden ve uyguladığından emin olunmalıdır.
- Dijital ortamda (çevrimiçi oyun oynarken, sosyal ağlarda gezinirken) çocukların tanımadığı kişiler tarafından sözlü olarak saldırıya uğraması durumunda önce ilgili platform üzerinden şikâyet edilmesi ve engellenmesi gerektiği sonra ise ebeveyni ile paylaşması gerektiği anlatılmalıdır.
- Çocukların şifrelerinin ebeveynler dışında kimseyle paylaşılmamasına özen gösterilmelidir.
- Çocukları internet üzerinden gelebilecek zararlardan korumak için, Aile ve Çocuk Profilinden oluşan Güvenli İnternet Hizmeti (https://www.guvenlinet.org.tr/) tercih edilebilir.

Çocukları güvende tutmak, kurallar belirlemek ve dijital ortamdaki davranışları hakkında eleştirel ve yargılayıcı olmayan tartışmalar yapmak önemlidir. Çocuklar eleştirel bir yaklaşımla yapılan sohbetlerden rahatsız olurlarsa, zorbalıkla karşılaştıklarında veya mahremiyetlerinin ihlali gibi çevrimiçi bir sorunla karşılaştıklarında ebeveynlerine bilgi verme olasılıkları daha düşük olacaktır. Bunlar, güvenli bir çevrimiçi dünyanın anahtarlarından bazılarıdır.

SOSYAL AĞLARDA GİZLİLİK

FACEBOOK

Kullanıcıların arkadaşlarıyla iletişim kurmasını ve bilgi alışverişi yapmasını amaçlayan bir sosyal medya aracıdır.
Kişilerin paylaştığı, kendileri hakkında girdikleri bilgiler de dâhil olmak üzere her türlü veri kayıt altında olmakta ve kişisel özellikler de göz önünde bulundurularak karşılarına benzer sayfalar çıkabilmektedir.

Facebook İçin Tavsiyeler:

- Profil tanımlamalarında açık adres, okul, yaş gibi kişisel bilgiler paylaşılmamalı,
- Kullanıcılar;

  Gizlilik Ayarları → Ayarlar ve Gizlilik Kontrolü → İnsanlar seni Facebook'ta nasıl bulabilir?

  bölümünden başka kişilerin arama sonuçlarında çıkmalarını engelleyebilir.
- **Ayarlar → Gizlilik Ayarları → Arkadaş Listeni Kimler Görebilir? → "Sadece Ben"**

  seçeneği seçilerek arkadaş listesinin görünürlüğü diğer kullanıcılara karşı kapatılabilmektedir. Arkadaş listesinin görünürlüğünün kapatılması listede bulunan kişilerin mahremiyetlerini koruyacaktır.
- "**Watch'taki Videolar**" bölümünde kullanıcının ilgisini çekebilecek olan farklı sayfalara ait videolar bulunmaktadır. Bu videolar arasında yapılan canlı yayınlar da yer almaktadır. Canlı yayınlar sohbet özelliği barındırmakta ve tanımadık kişilerden gelebilecek olumsuz içeriklere karşı dikkat edilmesi gerekmektedir.
- Küçük yaştaki çocukların şiddet, müstehcen, küfür gibi uygunsuz içerikleri barındıran fotoğraf ve video paylaşımlarına denk gelmesi ihtimaline karşı dikkat edilmeli, üye oldukları gruplar takip edilerek ebeveyn kontrolünde kullanılmalıdır.
- Paylaşılan içeriklerin güvenirliği mutlaka sorgulanmalı, doğruluğundan emin olunmayan paylaşımlar yapılmamalıdır.

INSTAGRAM

Instagram uygulaması fotoğrafların ve kişisel bilgilerin paylaşılabildiği bir mecradır.
Küçük yaştaki çocuklar neyi kiminle paylaşacakları konusunda yetkin değillerdir. Dolayısıyla paylaştıkları fotoğrafların kötü niyetli kullanıcılar tarafından kullanılıp kötü sonuçlar doğurabileceğini hesaba katamayacaklardır.

Instagram İçin Tavsiyeler:

- Hesabın gizlilik ayarlarının yapıldığından emin olunmalıdır.
  Ayarlar → **Gizlilik** → **Hesap Gizliliği** → **Gizli Hesap** seçilerek profil gizliliği aktif hale getirilmelidir.
- Tanınmayan bir cihazdan giriş yapılma ihtimaline karşı hesap şifresine ek olarak özel bir kod ile giriş yapabilmek için:
  Ayarlar → **Güvenlik** → **İki Faktörlü Kimlik Doğrulaması** özelliği aktif hale getirilmelidir. Bu özellik şifre bilinse dahi kullanıcı onay vermeden oturum açılmasına imkân vermeyecektir.
- Arama motorlarında yapılan sorgulamalara karşı, profil bilgileri kapatılmalıdır.
- **Ayarlar** → **Reklamlar** → **Reklam Konusu Tercihleri** bölümünden daha az görmek istenilen reklamlar düzenlenebilmektedir. Böylelikle kullanıcıların kişisel tercihlerine göre sakıncalı olabilecek içerikler gizlenebilecektir.

WHATSAPP

Whatsapp uygulaması, akıllı telefon kullanan kişilerin birbirlerine mesaj, görüntü, video ve ses klipleri göndermelerine izin vermekte, hatta telefon görüşmesi yapma imkânı da sağlamaktadır.
Whatsapp ile iletişim sadece bir kişi ile yapılabildiği gibi grup görüşmeleri de yapılabilmektedir.
Kişiler Whatsapp uygulamasına kaydolduktan sonra adres defterlerindeki whatsapp kullanıcılarını otomatik olarak görüp, hemen iletişime geçebilmektedir.

Whatsapp İçin Tavsiyeler

- Whatsapp hesabının gizlilik ayarları yapılmalıdır.
  - Gelen mesajların ekrandaki ön izleme özelliği gizlilik açısından kapatılabilmektedir.

iOS cihazlarda:

Ayarlar → **Bildirimler** → **Mesajlar** → **Önizlemeleri Göster**

Android cihazlarda ise cihaz markasına bağlı olarak değişmekle birlikte:

Ayarlar → **Mesajlar** kısımlarından değiştirilebilmektedir.

- WhatsApp uygulamasında

Ayarlar bölümünde; Hesap → **İki Adımlı Doğrulama ve Etkinleştir** seçeneğini aktif edip altı haneli şifre belirlenebilir ve iki adımlı doğrulama (2FA) özelliği kullanılabilir. Bu özellik ile başka kişilerin konuşmaları okuma ihtimalinin önüne geçilebilmektedir.

YOUTUBE

Youtube popüler bir video paylaşım uygulamasıdır. Youtube üzerinde videodan videoya gezinirken birçok uygunsuz içeriğe, şiddet, müstehcenlik, siber zorbalık ve birçok reklama maruz kalınabilmektedir. Bu nedenle, ebeveynlerin çocuğun psikolojik ve bedensel sağlığını korumak için Youtube uygulamasını işlevsel kullanmaları ve çocuklarını iyi yönlendirmeleri gerekmektedir.

YouTube İçin Tavsiyeler:

- Çocuklar Youtube platformu ile yalnız başlarına ve kontrolsüz bırakılmamalıdır.
- Youtube'un uzun süreli kullanımının çocukların fiziksel, duygusal, bilişsel ve sosyal gelişimlerine büyük zararlar verebileceği unutulmamalıdır.
- Sakıncalı içeriklere karşı Youtube "**Kısıtlı Mod**" etkinleştirilmelidir.

Hesap → **Ayarlar** → **Kısıtlı Mod** → **Etkinleştir**

- Olumsuz içeriklere sahip videolarla karşılaşma riskine karşı **Hesap** → **Ayarlar** → **Otomatik Oynatma** seçeneğinden otomatik oynatma özelliği kapatılabilir. Bu durumda izlenen video bitiminde başka bir video otomatik olarak devreye girmeyecektir.
- Ebeveynler çocuklarının yaşlarına uygun videolardan belirli oynatma listesi oluşturarak listeye aldıkları videoları izlemelerini sağlayabilirler. Belirli bir oynatma listesinin oluşturulması, çocukların olumsuz içeriklerle karşılaşmalarının önüne geçecektir.
- Youtube başında çok fazla zaman geçirmeye meyilli çocukların bu isteklerine ebeveynleri tarafından sınır koyulmalıdır.

TWITTER

Kullanıcıların güncel olayları ve haberleri takip etmek, anlık düşünceleri paylaşmak, bir olay veya kişiyi takip etmek gibi çeşitli amaçlarla kullandıkları bir sosyal ağdır.
Twitter, çocuklar tarafından çok fazla tercih edilmeyen bir mecra olmasına rağmen yine de genç yaşta kullanıcıları bulunmakta ve kullanıcıların karşısına şiddet içeren ya da pornografik içerikli paylaşımlar çıkabilmektedir.

Twitter İçin Tavsiyeler:

- Takip edilen hesaplara, paylaşılan ve beğenilen içeriklere dikkat edilmeli, kullanıcılar bu içerikleri silse dahi tamamen yok olmadığı, dijital dünyada birer ayak izi olarak kaldığı unutulmamalıdır.
- Kullanıcılar **Profil** → **Ayarlar ve Gizlilik** → **Gizlilik ve Güvenlik** → **Direkt Mesajlar** bölümünden karşılıklı olarak takipleşmedikleri kişilerden mesaj alımını durdurabilirler.
- **Gizlilik** → **Güvenlik Ayarları** → **"Tweet Gizliliği"** bölümünden **"Tweetlerimi Korumaya Al"** seçeneği ile paylaşımların yalnızca takip edenlerce görünmesi sağlanabilir.
- Farklı bir cihazdan hesaba giriş yapılması ihtimaline karşı e-posta ile bildirim aktif hale getirilmelidir.

TİKTOK

Uygulamanın kendi içinde yer alan popüler müziklerin kullanılarak kısa videolar çekilebildiği ve paylaşılabildiği sosyal medya platformudur.

TikTok platformunda kullanıcı oluşturan herhangi bir kişinin hesabı ilk etapta herkese açık olarak gözükmektedir. Bu da kişinin doğrudan korunmasız ve paylaştığı gönderilerin herkes tarafından görülebilmesi anlamına gelmektedir.

TikTok İçin Tavsiyeler:

- Çocukların uygun olmayan küfür veya müstehcen içerikler barındıran videolar ile karşılaşmaları ihtimaline karşı uygulama ebeveyn denetiminde kullanılmalıdır.
- Çocukların TikTok hesabı ebeveynleri tarafından takip edilmeli, yaş grupları için uygun olan hesapları takip ettiklerinden emin olunmalıdır.
- Paylaşılan videolara sadece tanıdık kişilerin ulaşabilmesi, yabancı kişilerden gelebilecek olan mesajlar ve yorumların engellenebilmesi için **gizlilik ayarları "özel"** olarak ayarlanmalıdır.
- Uygulama üzerinden konum bilgisi paylaşılmaması adına konum servisleri kapatılmalıdır.
- TikTok uygulamasında harcanan zamanı ve uygunsuz videoların kısıtlanmasını sağlamak amacıyla;
    - TikTok hesabının **sağ üst** kısmında bulunan **üç noktaya** basılması → şemsiye simgesinin yanında bulunan "**Dijital Refah**" yazısının seçilmesi gerekmektedir. Daha sonra "**Ekran Zaman Yönetimi"** ve **"Kısıtlı Mod**" seçenekleri tıklanarak açık hale getirilmelidir.

SNAPCHAT

Kullanıcıların anlık fotoğraf ve video çekip, bu fotoğrafları kısa notlar ve efektler ile renklendirerek paylaşabilme özelliği sunan bir sosyal medya aracıdır.
Paylaşılan fotoğraf ve videolar 1 ile 10 saniye arasında bir süreyle sınırlandırılmaktadır. Paylaşılan gönderiler, takipçiler tarafından görüldükten sonra 24 saat içinde kendi kendini yok etmektedir.

Snapchat uygulamasında paylaşılan gönderilerin bir kalıcılığı olmadığı için kullanıcılar kötü amaçlı da kullanabilmektedir. Genç kullanıcılar Snapchat'i kullanarak kendi aralarında uygunsuz ve şiddet içerikli fotoğraflar paylaşabilmektedir. Silindiği zannedilen görüntüler her an kullanıcıların karşısına çıkabilmekte ve siber zorbalık aracı olarak kullanılabilmektedir.

Snapchat İçin Tavsiyeler:

- Ebeveynler çocuklarını bilinçlendirmeli, yaptıkları paylaşımlara dair olumlu yönlendirme yapmalıdır.
- Ebeveynler, uygulamayı kullanan çocuklarına arkadaşlarından gelen görüntülerin onlara karşı siber zorbalık aracı olarak kullanmamaları gerektiğini uygun bir dille anlatmalıdır.
- Snapchat üzerinden özel fotoğraflarını paylaşmamaları gerektiği, farklı sonuçlar doğurabileceği anlatılmalıdır.
- Çocukların kimlerle iletişim kurdukları, kimleri takip ettikleri ebeveynler tarafından denetlenmelidir.
- Uygulama üzerinden konum bilgisi paylaşılmamalı, konum servisleri kapatılmalıdır.

İNTERNET YARDIM
www.internetyardim.org.tr

İNTERNET BİLGİ İHBAR MERKEZİ
ihbar web
www.ihbarweb.org.tr

Güvenli Web
www.guvenliweb.org.tr

Güvenli Çocuk
www.guvenlicocuk.org.tr

güvenli internet
www.guvenlinet.org.tr