Ebeveynler için Siber Güvenlik

Dijital Dünyada Kendinizi ve Çocuğunuzu Nasıl Güvende Tutarsınız?

TEKNOPARK İSTANBUL Mesleki ve Teknik ANADOLU LİSESİ

ÇOCUKLARIMIZ
#HerŞeyeDeğer

Ebeveynler için Siber Güvenlik

Dijital Dünyada Kendinizi ve Çocuğunuzu Nasıl Güvende Tutarsınız?

2024

İ S T A N B U L

Ebeveynler için Siber Güvenlik
Dijital Dünyada Kendinizi ve Çocuğunuzu Nasıl Güvende Tutarsınız?

1. baskı: 27 Ocak 2024

ISBN: 978-625-6736-73-3

Yazar:
Cafer ULUÇ
Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

Danışman:
Doç. Dr. Can EYÜPOĞLU
Milli Savunma Üniversitesi, Hava Harp Okulu

Son okuma:
Cem KARAKAYA
Münih Emniyet Müdürlüğü, Siber Suçlar Dairesi

Psikolojik danışmanlar:
Sevcan DUĞAN
Pelin DEMİRCİ
Vali Muammer Güler Sosyal Bilimler Lisesi

İçindekiler

İSTİKBAL GÖKLERDEDİR!

"Ebeveynler için Siber Güvenlik" kitabımızı,

Asırlık çınar Cumhuriyetimizin ikinci yüzyılında, bu çalışmanın hazırlandığı günlerde Türk Uzay Misyonu kapsamında Türkiye'nin ilk astronotu olarak görevlendirilerek gökleri yuvamız yapan Hava Pilot Albay Alper Gezeravcı ve mühendis Tuva Cihangir Atasever'e; köklerden göklere bağımsız, özgür, güvenli, eğitimde, ekonomide, sanatta ve bilimde öncü bir ülke için çalışanlara,

pusulası Ay Yıldız olanlara ithaf ediyoruz.

Giriş

Sayın Veliler,

Çağımızın belirleyici unsuru bilişim teknolojilerinin gerek bireysel gerek toplumsal gelişimin öncülüğünü üstlendiği günümüzde İnternet, bileğimizdeki saate, cebimizdeki telefona, mutfağımızdaki kahve makinesine, koridorumuzdaki aydınlatmaya, banyomuzdaki ısıtmaya, odamızdaki ses sistemine, evimizdeki robot süpürgeye değin girmiş durumda. Gündelik hayatın her alanında kendine böylesine yer bulan bu teknolojik çözümler, birtakım güvenlik ve mahremiyet sorunlarıyla birlikte çözümü güç olan tehditleri de karşımıza çıkarmaktadır. Bu bağlamda bu kılavuz kitap, geleceğimizin teminatı çocuklarımızın kendilerini özgür ve güçlü biçimde ifade edebilmelerine olanak tanıyan dijital dünyanın risklerinin farkına varmalarında ve onlara destek olmanızda sizlere yardımcı olabilmek adına hazırlanmıştır.

Siber uzayın zaman algısı fiziki dünyadan farklı bir yapıya sahiptir. Geleceği konusunda soyut düşünme, mantık ve muhakeme, çeşitli riskleri görme konusunda gelişmekte olan çocuklarımızın güvenli bir dünya için dijital ürün ve hizmetleri kullanırken bilinçli bir gelecek tasarlamalarında farklı perspektifler sunmak amacındayız. Nitekim çok açık ki içinde bulunduğumuz bu çağda, geleceği çocuklara bırakma geleneği de yalnızca onlar için değil onlarla birlikte bir gelecek tasarlanması gerekliliğini ortaya koymaktadır.

Memleketi asıl ışığa boğacak olan, geleceğin birer yıldızı çocuklarımızı fiziki dünyada olduğu gibi dijital dünyada da korumak, güvenli bir ortam sunmak için ebeveynlerin-öğretmenlerin-araştırmacıların ve kolluk kuvvetlerinin iş birliğinde çalışması, bütüncül yaklaşımla tüm unsurların bir aradalığı temel olmalıdır.

Bu kitap, çocuklarımıza yönelik gördüğümüz sorumluluk ölçüsünde siz ebeveynlere yönelik nasıl yardımcı olabileceğiniz bilgisini ayrıntılı olarak vermek adına ele alınmıştır. Kutlu olması dileğiyle!

Önce Söz

Değerli Anne ve Babalar,

Teknoloji eğitimden sağlığa, gıdadan ulaşıma, politikadan kültürel yaşama, finansal sistemlerden ulusal güvenliğe varıncaya kadar varlığını ortaya koyan bir yapıdadır. Kapsayıcılığının ve etki düzeyinin bu denli geniş olması, teknolojiye karşı değil teknolojiyle uyum içerisinde hareket etmeyi, tüketen bir konumdan üretici ve oyun kurucu bir pozisyonda eyleme geçmeyi gerektirmektedir. Nitekim Atatürk'ün işaret ettiği o *muasır medeniyetler seviyesinin de üstüne* çıkmanın yolu, zamanın ruhunu yakalamaktan geçmekte ve buradan hareketle de önceliklenen olarak 21. yüzyıl becerilerini edinmek ve edindirmek üzerine bir yaklaşımın esas alınması ortaya çıkmaktadır.

Yarının bürokratı, diplomatı, komutanı, savcısı, yöneticisi, astronotu, mühendisi, iş insanı, öğretmeni, sanatçısı sizlerin çocukları olacak. Öyleyse bu bilinçle hareket edebilmeli ve onlar henüz birer çocukken arkalarında bıraktıkları dijital ayak izlerinin farkında olmalıyız. Bunu gerçekleştirebildiğimiz ölçüde onlar hakkında bilgi toplayan ve zamanı gelinceye kadar kendi çıkarları adına bu verileri saklayan sistemlere karşı koruyabiliriz. Anımsanmalıdır ki günümüzün yeni petrolü veridir. *Veriye hükmeden, tüm unsurlara hükmeder* yaklaşımı otoriteler tarafından uygulanmaktadır. Ve yüzyıllardır değişmeyen bir netlikte, güçlü olanın ahlaki yaklaşımları ve yasal kuralları kendisine hizmet ettiği ölçüde esnetebildiği de göz ardı edilmemelidir.

Bilinir ki hepimiz, zincirdeki o en zayıf halka kadar güçlüyüzdür ve o zayıf halka, tüm zincirin dağılmasına neden olabilir. *Hepimiz güvende olmadan, hiçbirimiz güvende değiliz.* Buradan hareketle bir Harbiyeli yaklaşımıyla geride kimseyi bırakmadan ilerleme ilkesini benimsemeli, birlikten doğan güçle *çalışmaların en yükseği olanı için, bağlı bulunduğumuz toplum için çalışmayı* önceliklemeliyiz. Bu bağlamda ülkemizin ilk ve tek siber güvenlik lisesi Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi olarak üstlendiğimiz

ödevlerden biri de İnternet'in özgür ve güvenilir bir yapıda olması için çözümler sunmak, toplumun her bireyinin bilinçli ve güvenilir teknoloji kullanıcısı olmasına yönelik içerikler hazırlamaktır.

Yukarıda sözü edilen bu amaç, aynı zamanda Anayasamızın 41. maddesi gereği kamusal bir gereklilik de içerir: "*Devlet, her türlü istismara ve şiddete karşı çocukları koruyucu tedbirleri alır."* Bununla birlikte T.C. Ulaştırma ve Altyapı Bakanlığınca yayınlanan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)" çerçevesinde *siber güvenlik farkındalığının tüm toplumda üst seviyede tutulmasına yönelik etkinliklerin sürdürülmesi* ile *çocukların siber ortamda korunmasının sağlanması* başlıkları, ilgili belgede ulusal siber güvenlik hedefleri arasında önemle vurgulanmaktadır.

Vali Muammer Güler Sosyal Bilimler Lisesinde 7 Aralık 2023'te Veli Akademisi kapsamında ebeveynlere yönelik gerçekleştirdiğimiz seminer sonrası bir gereksinim olarak ortaya çıkan bu kılavuz kitapta velilerin görüşleri de dikkate alınarak uygulanabilir öneriler olmasına özen gösterilmiştir. Yalnız önerilerle yetinilmemiş, kapsayıcı bir bakış açısıyla güvenli bir çevrim içi disiplini önceliklenmiştir. Her şeyden önce gözümüzden sakındığımız çocuklarımız için, toplumumuz için dijital dünyanın olası risk ve tehditlerinden korunabilmek, olası fırsat ve olanaklarından güvenli biçimde yararlanabilmek adına ve *kendine yeterlilik ilkesi* doğrultusunda tüketici konumdan üretici bir konuma erişebilmesi amaçlanmıştır.

"Ebeveynler için Siber Güvenlik – Dijital Dünyada Kendinizi ve Çocuğunuzu Nasıl Güvende Tutarsınız?" adlı kitabımızın dijital okuryazarlık, bilinçli ve güvenli İnternet kullanımının bir kültür olarak güçlenmesi kapsamında yararlı olmasını diler, bu çalışmanın ortaya çıkmasında katkı ve katılım sağlayan tüm paydaşlara esenliklerimi iletirim.

Cafer ULUÇ
Milli Savunma Üniversitesi
İstanbul, 6 Ocak 2024

Küçük hanımlar, küçük beyler!

Sizler hepiniz geleceğin bir gülü, yıldızı, geleceğin ışığısınız. Memleketi asıl ışığa boğacak sizsiniz.

Kendinizin ne kadar önemli, değerli olduğunuzu düşünerek ona göre çalışınız.

Sizlerden çok şeyler bekliyoruz.[1]

[1] *19 Ekim 1922'de Bursa'da kendisini karşılayan çocuklara hitaben söylemiştir.*

Karşılama

Doç. Dr. Can EYÜPOĞLU
Milli Savunma Üniversitesi, Hava Harp Okulu,
Bilgisayar Mühendisliği Bölüm Başkanı

———

Sayın Ebeveynler,

Günümüzde dünyamız dijitalleşmiş ve siber güvenlik de bu dünyanın ayrılmaz bir parçası haline gelmiştir. İnternet ve yeni teknolojiler hayatlarımızı oldukça kolaylaştırmış ancak bu imkanların yanında birçok tehlikeyi de beraberinde getirmiştir. Çocuklarımızın bu dijital dünyadaki tehditlere karşı korunması en büyük sorumluluklarımızdan biridir.

Bu kitabın temel amacı, siber güvenlik kavramını anlaşılır bir şekilde ele alarak anne ve babaların dijital dünyadaki tehlikeleri tanımalarını sağlamak ve bu tehlikelere karşı önlem almalarına yardımcı olmaktır. İnternet'in sunmuş olduğu fırsatlardan yararlanırken çocuklarımızın dijital dünyada karşılaşabilecekleri potansiyel risklere karşı bilinçli ve tedbirli olmak bir zorunluluk haline gelmiştir. Oyunlar, sosyal medya ve diğer dijital platformlarla ilgili mahremiyet ve güvenlik endişelerini anlamak, anne ve babaların çocuklarını korumalarında kritik bir rol oynamaktadır.

Kitap, siber zorbalık kavramından ve türlerinden bahsetmenin yanı sıra siber zorbalığa maruz kalındığında ebeveynlerin neler yapması gerektiği konusunda öneriler sunmaktadır. Ayrıca, kitapta dijital dünyada var olan olası risk ve tehditlere karşı alınabilecek tedbirler hakkında önerilere de yer verilmektedir. Bu kitabın siber güvenlik konusunda farkındalık yaratmanın yanı sıra ebeveynlerin ve özellikle çocuklarımızın dijital dünyada güvenli bir şekilde bulunmalarına yardımcı olması dileğiyle.

İstanbul, 21 Ocak 2024

Sunuş

Cem KARAKAYA
Münih Emniyet Müdürlüğü, Siber Suçlar Dairesi Müdürü

———

Dijital dünyalar, dijital beceriler gerektirir.

Ailemin beni yetiştirirken ve bana iyi bir insan olmamı öğretirlerken yaşadıkları problemler veya ilgilenmeleri gereken alanlar ile bugünkü aile fertlerinin yaşadıkları problemler ve alanlar arasında dağlar kadar fark var. Annemin bana sürekli söylediği "Oğlum, televizyona bu kadar yakından bakma, gözlerin bozulur." cümlesi hala kulaklarımdadır. Annem için önemli olan bir şey daha vardı: "Benim oğlum neye bakıyor?". Ailemin teknoloji ile ilgili endişeleri tamamıyla bundan ibaretti. Bir de telefon çıktıktan sonra, telefona kilit koyarlardı ki arkadaşlarımla uzun konuşmalar yapmayayım diye.

Ama teknolojinin çok hızlı gelişimi ile ortaya çıkan yeni sorunlar ve yeni alanlar günümüzdeki aile fertlerini zor duruma düşürdü çünkü bizler, bugünkü aile fertleri olarak, bu dijital becerileri çocuklarımıza nasıl vereceğimiz konusunda ne bir bilgi sahibiyiz ne de bunun nasıl yapılabileceğini ailelerimizden öğrendik. Bu konudaki tecrübeleri edinebilecek ilk nesil biziz. Pek tabii ki bu konuda yardıma ihtiyacımız var ve bu yardımı en iyi şekilde bu türdeki kitapları okuyarak ya da her ne kadar büyük tehlikeler de içerse güzel bir ortamdan alabiliriz: İnternet.

Şahsım yurt dışında yaşasa da bugünkü teknolojik imkanlar sayesinde, Türkiye'de bulunan ailem torunlarını neredeyse her akşam görme imkanına sahipler veya aynı konuda yardıma ihtiyacı olan insanlar, sosyal ağlar sayesinde karşılıklı olarak birbirlerine yardım edebilme ve tecrübe değiş tokuşu yapabilme imkanına sahip olabilmektedirler. Ne kadar hoş ve ne kadar güzel… Ama aynı sosyal

ağlar insanları zorbalıklarla yaşama sevincinden de uzaklaştırabilmektedir. Şimdi sosyal ağlar mı tehlikeli yoksa bunu kullanan insanoğlu mu?

Etik ve terbiye günlük yaşantımızda ne kadar önemliyse bir o kadar da İnternet ve sosyal ağlar kullanımında da önemlidir. Aile fertleri olarak bu kadar önemli becerileri çocuklarımıza verebilmek için öncelikle kendimizi bilgilendirmemiz gerekmektedir. Bilinmesi gereken en önemli konular şundan ibarettir:

- Türk Ceza Kanunu'nda işlenen her konu, İnternet ve sosyal ağlar için de geçerlidir.

- Akıllı telefonlar, bir cep telefonu değil bir bilgisayardır.

- Çocuklarımızı dışarıda karşılaşabilecekleri tehlikelere karşı nasıl hazırlıyorsak aynı hazırlığı İnternet ve kullanımı konusunda da yapmamız gerekmektedir.

- Çocuklarımıza iyi bir örnek olabilmemiz için aile rolümüzü unutmamamız lazımdır.

Bir aile ferdi olarak çocuklarımızı 24 saat kontrol altında tutabilmemiz imkansız olsa da teknoloji sayesinde veya örneğin akıllı telefonların sunduğu ayarlar sayesinde çocuklarımızı bazı içeriklerden uzak tutmamız mümkündür. Ama en önemlisi, sizin ve çocuğunuz arasındaki iletişim ve güvendir. Çocuğunuz, karşılaştığı her problemde size geliyor ve yardım talebinde bulunabiliyorsa ve siz buna zaman ayırabiliyorsanız büyük bir işi başardınız demektir. Günümüzdeki en büyük problemlerden bir tanesi de şu değil midir: *Bir gün içinde bir ekrana toplam bakma süremiz, sevdiğimiz kişilerin gözlerine bakma süresinden daha fazladır.*

Bu kitabın siz aile fertleri için güzel bir yardımcı kaynak olabilmesi dileğiyle saygı ve sevgilerimi sunarım.

Münih, 12 Ocak 2024

Başlarken

Sayın Veliler,

Her ailenin kendine has bir yapısı vardır ve bilinir ki ihtiyaç ve yaklaşımlar da bu ölçüde esneklik gösterir. Bu kitapta yer alan içerikleri uygularken bu doğrultuda özelleştirme yapılmasında fayda görülmektedir. Nitekim ailenizin iç yapısını ve çocuğunuzu en iyi sizler tanıyabilirsiniz. Anımsanmalıdır ki çocuk için ilk okul ailesi, ilk öğretmeni ise anne ve babasıdır.

Bilişim teknolojilerinin gelişim ve değişim hareketliliği göz önüne alındığında işbu çalışmada yer alan ifadeler, öneriler ve yaklaşımlar süreç içerisinde gereksinimlere bağlı olarak güncellenmeye ihtiyaç duymaktadır.

Kamuya açık biçimde dijital ortamda yayınlanan bu çalışmada sizlerden gelecek aktif bildirimlerle içeriğin güncel tutulmasında katılım ve katkılarınızı bekleriz.

Güven/lik Algısı

Hepimiz, güvende olduğumuzu düşünürüz. Dahası, öyle olduğunu düşünmek isteriz çünkü güvende olduğumuzu düşünebilmenin kendisi bile bizi güvende hissettirir. Nitekim güven, insanın doğası gereğidir ve insan –yalan da olsa– inanmak ister.

Bu durum, yapısal olarak bir insana özgü bir normdur. Aksi takdirde sürekli bir savunma halinde olsak bu acıyı yüreğimiz kaldıramayabilirdi. Sürekli bir tehdit altında olan zihnimiz verimli çalışamaz; sürekli aklımızı meşgul eden bu düşünceden kopamaz, donakalırdık. Televizyon ve sosyal medyanın neden sürekli korku yaymaya yönelik haberleri bizlere yönelterek bir maruz bırakma yolu seçtiğini anlamak bu açıdan bakıldığında daha bir şeffaflık kazanıyor. Maslow'un İhtiyaçlar Piramidi'nden de bildiğimiz üzere güvenli hissedemediğimizde geriye kalan hiçbir unsura da yer kal(a)mıyor hayatımızda.

Uyuşturucuyla mücadele olduğu gibi bağımlılığın ve güvenliğin her türlüsüyle mücadelede kolluk kuvvetleri bir başına yeterli görülmemelidir. Çocuklarımızı kötü insanlardan ve kötülüklerden korumak için hep birlikte hareket edebilmeli, iş birliği içerisinde olabilmeliyiz. Unutmamalıyız ki anne ve babanın yerini hiç kimse dolduramaz. Hiç kimse sizler kadar çocuklarını tanıyamaz, sevemez, anlayamaz. Gerek güvenlik güçlerimiz gerek araştırmacı ve öğretmenler olarak bizler siber dünyada güvenliği sağlamak adına çalışırken siz anne ve babalar da çocuklarınızı gözetlemeli, onları her koşulda ihmal etmemelisiniz. Evde huzurlu bir yuva hisseden birey, mutluluğu dışarıda bir yerlerde aramaya hevesli olmaz.

Güvenlik, olay yaşanmazdan önce anlam kazanmaktadır. Önleyici faaliyet olarak yaklaşılması gerekir. Okuma yazmada gösterilen hassasiyet, dijital okur yazarlığı da içine alacak biçimde zaman ve emek verilmelidir. İstanbul gibi metropol kentlerinde türlü profillerde insanlar var. Koca koca apartmanlarda yaşıyor, karşı komşumuzu dahi

tanımıyoruz. Peki, çocuklarınız telefonlarıyla, tabletleriyle, oyun konsollarıyla, bilgisayarlarıyla baş başayken onları tanımadığınız kişilere karşı nasıl güvende tutabilirsiniz?

Teknoloji, potansiyel olarak fırsat ve tehditleri içinde barındırır. Bu yönüyle doğrudan bireyi ve toplumsal yapıyı hem kalkındırmada hem de yıpratmada etkili bir araca dönüşebilmektedir. Peki, iki yönü de böylesine baskın olabilen bir mecrada şu soruyu siz de sordunuz mu kendinize: *Kimin bende ne işi var?*

Bilişim teknolojilerinin ve İnternet'in içinde doğan bebekler henüz konuşamadan telefon ve tablet gibi mobil cihazlarla tanışmakta ve kullanabilmektedirler. Çocuğun her dijital temasıyla birlikte arkada bırakılan her etkileşimle oluşan dijital ayak izleri sonucunda elde edilen büyük veri doğrultusunda özel hayatı, kişisel verileri ve bunların bir çıktısı olarak karakterinin tanınması ve analiz edilmesine olanak tanınmaktadır.

Peki, bu alt başlıktaki ifade size de tanıdık geliyor mu?

"Kimin bende ne işi var?"

1984 yılında Rockwell ve Michael Jackson'ın düetini üstlendiği "Somebody's Watching Me" şarkısında şu sözler geçer:

> *Ben sadece sıradan bir hayatı olan sıradan bir adamım.*
> *Dokuzdan beşe kadar çalışıyorum.*
> *Tek istediğim evimde yalnız kalmak.*
> *Hep biri beni izliyormuş gibi hissediyorum.*
> *Ve hiç mahremiyetim yok.*
> *Söyle bana, bu sadece bir rüya mı?*

Birçoğumuz bu şarkıdaki gibi sıradan hayatlara sahibiz. Şöyle bir baktığımızda bizim gibi hayatları olan milyonlarca insan da var. Gerçekten de *kimin bende ne işi olabilir* sorusu bu açıdan oldukça mantıklı görünüyor olabilir. Cem Yılmaz'ın şu meşhur güldürüsünde

olduğu gibi muhtemelen CIA ya da MİT de peşimizde değildir. Sonuçta gizli ve sakıncalı konular konuşmuyor, gündelik koşuşturmaca içerisinde stres atmak için video izliyor, araştırma yapmak için makale okuyor ya da mutfak alışverişi için sipariş geçiyoruzdur. İşte, yalnızca bu üç davranışın bile kendimiz hakkında ne gibi analizler çıkarılabileceğini bilen şirketlerin bizde işi oluyor. Onlar için bireyselde kim olunduğunun bir önemi yok. Adınızın ne olduğuyla değil verilerinizle ilgileniyorlar. Nitekim günün sonunda arkada bırakılan her dijital ayak izi, en iyi ihtimalle, birer ticari faaliyete dönüşebiliyor.

Dolayısıyla evet, biri veya birileri bizi çoğu zaman gözetlemese de takip ediyor. Dijital ayak izlerimizin değmediği alan yok denecek kadar azalıyor. Çok değil, on yıl öncesine kadar ailemize söylemeye çekindiğimiz kişisel sırlarımızı WhatsApp'te arkadaşlarımızla paylaşıyoruz. Böylesi bir *nimeti* kaçırmak istemeyenler pekçedir. George Orwell'ın 1948'de kaleme aldığı 1984 romanında olduğu gibi bir gözetim toplumu içerisinde olmadığımızı yok saymak var olan gerçekliği ortadan kaldırmayacağı gibi bizlerin direncini de zayıflatıcı bir yaklaşım olacaktır.

Evet; kurum, kuruluş ve şirketler sizin kim olduğunuzla ilgilenmiyor. Pazarda meyve satan manav da olabilirsiniz, serbest zamanlı çalışan bir grafiker de olabilirsiniz. Bunun yanı sıra bir ebeveyn olarak çocuğunuzu olası bir kariyer ve gelecek planı bekliyor. Şu an sizin ya da öğretmenlerinin gözünde pek de parlak bir öğrenci olarak görünmüyor olabilir. Oysa daha önünde yıllar var. Bir kişinin aktüelde olan durumundan ötede potansiyelde taşıdıkları önemlidir. Ülkeyi yöneten bürokratlar, bilim üreten araştırmacılar ve kritik noktalardaki kişiler… Kimisi yan komşunuz, kimisi akrabanız, kimisi adını dahi duymadığınız bir mahalleden çıkacak. Bu görevlerden birinde de sizin çocuğunuz olabilir. Doğumumuzdan beri içli dışlı olduğumuz bu siber dünyada yaptığımız her hareket dijital bir ayak izi olarak kalıyor. Şu an Türkiye'nin herhangi bir yerinde, örneğin Beylikdüzü'nde ya da Samsun'da bir öğrenci geleceğin hakimi,

savcısı, üst düzey bir komutanı, cumhurbaşkanı olacak. Lise boyutunda yaklaşırsak örneğin sosyal bilimler liselerinin amacı bürokrat ve akademisyenler yetiştirmektir. Diğer lise türlerine baktığımızda da her tematik alandaki eğitim kurumlarımızın kendilerine özgü amaçları bulunmaktadır. Dolayısıyla geleceğimizin tüm mesleklerinde görev üstlenecek kişiler sizlerin çocukları arasından çıkacaktır. Buradan hareketle kimsenin sizinle bir işi olmayabilir ancak çocuğunuzla olabilir.

Peki, herkes üst düzey bir makamda olamayacağına göre gerçekten de *kimin bende ne işi olabilir ki?* Örneğin, Çankaya Belediyesi'nde çalışan bir memur olun. Bilinçli bir kullanıcı değilseniz tüm belediyenin -ve dolayısıyla vatandaşların- siber güvenliği tehlikeye girebilir. Ya da bir lisede görevli bir öğretmenin okul bilgisayarına takacağı USB bellek tüm okulu riske sokabilir. Güncel bir örnek olması açısından: 22 Kasım 2023'te BAYKAR'ın İHA üretim fabrikasında çalışan bir stajyerin 4 harddisk çaldığı ortaya çıktı. Yakalayan ise çıkışta kontrolü sağlayan bir güvenlik görevlisiydi. Anımsayalım: *Hepimiz, zincirdeki zayıf halka kadar güçlüyüzdür.* O güvenlik görevlisi işini iyi yapamasaydı Türk Silahlı Kuvvetleri'nin ve Emniyet Teşkilatı'nın da envanterinde yer alan insansız hava araçlarına yönelik birtakım bilgiler karşı istihbarat örgütlerine veya teröristlerin eline geçecekti.

Yeni petrol, veridir. Bu noktada büyük veri kavramını irdeleyerek ücretsiz olarak sunulan hizmetlere farklı bir pencereden bakılacaktır. Dünyanın en iyi yazılımcı ve mühendislerinin geliştirdiği sistemler neden ücretsiz olarak son kullanıcıya sunuluyor? Bir Türk atasözü der ki: *Bedava peynir fare kapanında olur*. Nitekim bir ürün/hizmet ücretsiz ise orada sermaye bizler (veriler) oluyoruz. *Veri, yeni petrol.* Üstelik, petrol gibi tükenmiyor; dahası, veri arttıkça değerleniyor.

Büyük veri, toplumsal medya paylaşımları, ağ günlükleri, bloglar, fotoğraflar, videolar, işlem kayıt dosyaları gibi değişik kaynaklardan toparlanan yapısal olan veya olmayan tüm verinin, anlamlı ve

işlenebilir biçime dönüştürülmüş biçimine denmektedir. Bir başka açıklamaya göre ise büyük veri; sosyal medya paylaşımları, GSM operatörlerinden elde edilen arama kayıtları, fotoğraf, video, blog ve log dosyaları gibi farklı kaynaklardan elde edilen verilerin anlamlı ve işlenebilir hale dönüştürülmüş biçimidir. Artan bu paylaşımlar sadece bizim bireysel özelliklerimizi değil, paylaşım serileri yardımıyla toplumsal perspektifimizi de ortaya çıkarıyor. Ağa katılan farklı bireylerin üstlendikleri rolleri, davranış kalıplarını ve gizli özelliklerini ayıklamak amacıyla uygulanan analiz tekniğine Sosyal Ağ Analizi (SAA) denilmektedir. SAA iletişim, paylaşım, organizasyon, istihbarat, güvenlik gibi birçok alanda etkin olarak kullanılmakta olup bireysel analiz ve toplumsal analiz olmak üzere iki türlü bulunmaktadır. En nihayetinde her birey toplumun bir parçasıdır ve parçalar birleşince bütüne ulaşılabilmektedir.

Milyonlarca durum güncellemesi, fotoğraf, video… Sayı arttıkça istatistik açıdan yarar sağladığını belirtmek gerekir. Bu, kişisel analizden daha ziyade toplumun, topluluğun eğilimlerini, tepkilerini ölçmek için muhteşem bir araçtır.

Takip eden sayfalarda yaşanmış gerçek olaylar sıralanacaktır. Bazı konuların konuşulması, okunması dahi insanı rahatsız edebilir. Bu vakalardaki durumların benzerlerini yaşamamak adına önleyici güvenlik yaklaşımlarını ciddiyetle ve temelde ailece almak gerekir. Var olan gerçekleri reddederek onlar yokmuş gibi davranamayız.

Öyleyse şimdi de kimin sizde ne işi olabileceğine bir örnekle uzak bir kıtaya misafir olarak vakaları inceleyelim:

Sizde İşi Olanlar #1:
Avustralya Polis Okulu'nun 2011 mezunlarının yemin töreninde, polis rozetlerine kavuşan sevdiklerini izleyen ailelerin arasında bir adam göze çarpıyordu. Elindeki profesyonel kamerası, uzağı büyüten mercekle dikkat çeken bu adam, sırayla tüm mezunların yüzlerini fotoğraflıyordu. Gözaltına alınmasının ardından yapılan sorguda, polisler bu fotoğrafçının aslında organize suç örgütü olan bir

motosiklet çetesi mensubu olduğunu öğrendi. Suç örgütü adına çalışan adam, diğer suçlu dostlarının gelecekte olası bir gizli operasyon olması halinde içlerine bir polis sızdığında fark etmesi için fotografik yüz tanıma veri tabanı oluşturmak istiyordu.

Sizde İşi Olanlar #2:
Daha çok pedofililerin peşine düştükleri çocuklarda yaş, cinsiyet, saç rengi, boy gibi çok çeşitli tercihleri olduğu düşünüldüğünde, sosyal medya veya diğer çevrim içi kaynaklara yüklenen fotoğraflar, kendine kurban arayan bu çocuk istismarcıları için sanal dünya bir pazardaki alışveriş kataloğuna dönüşüyor. *Kimin bende ne işi var*, cümlesini pek rahatlıkla söyleyenler içlerini rahatlatmak istiyorlar ama tatsız da olsa bu konuları ele almak gerekir: Bugün TikTok, Snapchat ve Instagram gibi platformlar sapıkların bir numaralı bilgi toplama aracı olarak kullanılmaktadır.

Bir musibetin bir nasihatten evla olduğunu atalar yüzyıllar önce ifade ettiler. Bazı musibetler geri dönüşü olmayan, yıkıcı sonuçlar doğurabilmektedir. Buna sonu iç açıcı olmayan bir örnek Avustralya'da yaşandı:

Sizde İşi Olanlar #3:
Her birimizin hiç tanışmadığı yüzlerce arkadaşa sahip olduğu sosyal medya platformlarında o istekleri aslında kimin gönderdiği üzerine iyice düşünmekte yarar olabilir. Christopher Danevig isimli bir adam, Facebook'u, Sidney, Avustralya'da yaşayan on sekiz yaşındaki kurbanı Nona Belomesoff'u bulmak için kullandı. Kendisiyle iletişime geçmeden önce profili üzerinde titizlikle çalıştı. Belomesoff'un profilinde sürekli hayvan sevgisine dair iletiler paylaşması, sapığına, kendisiyle buluşmak için genç kızı ikna etme konusunda fikir vermişti. Nona'nın kendi isteğiyle paylaştığı sosyal medya verilerini kullanarak Dannevig, "James Green" adında sahte bir profil oluşturdu ve yerel bir hayvan kurtarma barınağının işe alım sorumlusu olarak çalıştığını söyledi. Sapık, genç kızı kandırmak için profilde bulduğu tüm bilgileri kullanmıştı. Sahte profili oluşturduktan

sonra Dannevig, Belomesoff ile bir süre mesajlaştı ve sonunda arkadaş olarak güvenini kazandı. Bundan kısa bir süre sonra ise çalıştığını iddia ettiği hayvan barınağında genç kızın tam da aradığı türden bir iş olduğunu duyurdu. Belomesoff, mülakat için adamla buluşmayı kabul etti. Sapığı ise genç kızı Sidney'in uzak bir bölümünde yer alan hayvan barınağına götürmeyi önerdi. Tutkuyla bağlı olduğu hayvanlarla çalışırken maaş alabileceği bir iş bulmanın heyecanına kapılan genç kız, adamla yolculuğu kabul etti. Sidney'in terk edilmiş kenar mahallelerinden birinde Nona'nın cansız bedenine ulaşıldı.

Sizde İşi Olanlar #4:
Eski günlerde bir hırsız, belirli bir evi hedef aldığı zaman, ev sahiplerinin tatilde olduğunu gösterecek geleneksel işaretler arardı: Kapının önünde biriken gazeteler veya akşamları açılmayan ışıklar ev sahibini ele verebilirdi. Ancak en basit hırsızlar bile araçlarını modern bir hale getirip hedeflerini ve girecekleri evi belirlerken teknolojiyi daha fazla kullanmaya başladı. Bu suçlular, her geçen gün artan bir şekilde Facebook, Snapchat, TikTok, Discord, Instagram ve X (Twitter) gibi sitelerdeki iletilerinizi arıyor, tıpkı iyi satışçılar ve pazarlamacılar gibi uzun vadeli kazançları için bıraktığınız verileri kullanıyor.

Bunun bir örneğine 2010'da New Hampshire, Nashu'daki bir grup yerel suçlunun, hedeflediği kişilerin evde olmadığını belirlemek için Facebook kullanmasıyla rastlanıldı. Nashua polisi bu suç şebekesinin soygun serisi sırasında elliden fazla eve girip yaklaşık 200.000 dolar değerinde mal çalmadan önce, hedeflerinin Facebook profillerini takip ettiğin keşfetti. Bunlar, dedelerimizin zamanındaki soyguncular değil. Daha fazla suç işlemek için teknolojiye hepimizden daha fazla uyum sağlıyorlar.

İngiltere'de hüküm giyen soyguncular arasında 2011'de yapılan bir çalışmaya göre, hapistekilerin %78'i bir ev belirlemeden önce Facebook, X ve Foursquare'i yakından takip ettiğini belirtiyor. Aynı zamanda girilecek evin olduğu bölgeyi incelemek ve suç mahallinden

kaçış rotaları belirlemek için de Google'ın *Street View* özelliğini kullanıyorlar. Sonucunda ise suçluların, bile isteye arkamızda bıraktığımız verileri bize karşı nasıl kullandığı ortaya çıkıyor.

Hırsızların sizi hedef alırken kullandığı yöntemlerden bir diğer ise İnternet'e yüklediğiniz dosyalara gömülen konum verileri. Indiana, New Albany'de yaşayan Keri McMullen ile Kurt Pendelton, evlerindeki plazma televizyon ile ses sistemini satmaya karar verdi ve ürünlerin fotoğrafını İnternet'e yükledi. Genç çift birkaç gün sonra, cumartesi akşamı yakınlardaki Louisville'de sahne alacak bir grubun konserine gideceklerini de Facebook'tan duyurdu. Aradığı elektronik cihazları çalmak için hırsızların bilmesi gereken her şey sağlanmıştı artık. Suçlular, ev sahipleri saatlerce konserde olacağı için hiç acele etmelerine gerek olmadığının da farkındaydı. Nihayetinde, çiftin evinden bir düz ekran televizyon, iki dizüstü bilgisayar, tüm teçhizatlarıyla birlikte bir ses sistemi ve nitelikli bir dijital kamera çalındı.

Sizde İşi Olanlar #5:
Bir zamanlar seyahat acentelerine, gazetelere ve plak şirketlerine ödediğimiz paralar, bize "World Wide Web"i getiren cömert insanlar sayesinde ortadan kalktı. Ancak bir saniye durup da Google'ın size neden hiç fatura göndermediğini merak ettiniz mi? Bu şirketler bize e-posta, haber, video ve fotoğraflarımızı koyacak bir alan gibi oldukça değerli hizmetleri yine *ücretsiz* bir şekilde sunarken karşılığında biz de onlara kendimize dair *birazcık* bilgi veriyoruz.

2004'te sunulan Gmail, kullanıcılarına 1 GB depolama alanı sunarak, sadece 2 MB alan sunan dönemin lideri Microsoft Hotmail'in yanında krallara layık gibi görünüyordu. Devasa bir depolama alanıyla birlikte kusursuz çalışma bir deneyim sunan Google hem kişisel hem de profesyonel e-postalarımıza erişim sağladı. Artık Google sadece aradığımız her şeyi değil; kime, ne yazdığımızı da öğrenebiliyordu. Google, mesajlarımızı tarayıp elektronik olarak okuyarak reklam

verenlere sunabileceği yepyeni bilgiler elde etti ve bize dair elinde tuttuğu profili genişletirken reklam ücretlerini de arttırdı.

Örneğin pek masum olarak annenize, sevdiğinizden ayrıldığınız için kendinizi kötü hissettiğinizi anlatan bir e-posta gönderdiğinizde, Google da size bir antidepresan, komedi filmi veya Karayipler'de bir tatil önerebiliyordu. Gmail'de çevrim içi kaldığınız sürece, tüm aramalarınızı takip edip bütün bunları size özel profiline ekleyebiliyordu. Sonuç olarak Google'ın size dair topladığı veri boyutu büyüdükçe şirket de büyüdü. Google, Android işletim sistemini ortaya çıkardı ve *yine ücretsiz* olarak dağıttı. Karşılığında ise akıllı telefonunuzu götürdüğünüz her yerde sizi izleme gibi bir ayrıcalığa sahip oldu.

Amerika'da bir başsavcı tarafından 2013'te açılan bir dava sonucunda Google, yüksek teknolojili 360 derece tavan kameralarıyla sokaklarda gezen garip görünümlü *Street View* araçlarının mahallelerimizde dolaşırken sadece şirketin *Street View* harita ürünü için fotoğraflar çekmediğini, aynı zamanda evlerimiz ve ofislerimizden, masum kullanıcıların bilgisayarlarının içinden parolalar, e-postalar, fotoğraflar, sohbet mesajları ve diğer kişisel bilgileri çaldığını itiraf etti. Apple da masum değil elbette. Siri ile konuşulan her kayıt analize tabi tutuluyor. *Touch ID* ile parmak izleri profilleştiriliyor. Instagram'ın envanteri, sizin ve benim kişisel verilerimizden oluşuyor. Bu veriler ise dünyanın her yerindeki şirketlere tekrar tekrar satılıyor.

Sosyal şebeke haritası oluşturularak kişilerin ilgi alanları, dostları, dahil olduğu grupları, istekleri, inançları, düşünceleri ve faaliyetleri ile ilgili bilgi toplanmaktadır. Örneğin Google, her web aramasını IP adresi üzerinden 18 ay süre ile saklar. Google sayfaları bilgisayarınıza yüklediği çerezler (cookies) ile sizin bilgisayar kullanma alışkanlıklarınızı, ne okuduğunuzu, hangi siteleri gezdiğinizi takip eder ve böylece profiliniz çıkar. ABD İç Güvenlik Bakanlığı (DHS), açıkça ifade ettiği gibi bu bilgileri bazen resmen isteyerek bazen sorarak kullanmaktadır.

Sizde İşi Olanlar #6:
Cep telefonunuzla bir fotoğraf çektiğinizde, konum verileri de (GPS koordinatları) görüntü dosyasının içine kaydedilir. Siz o fotoğrafları ve videoları Flickr, YouTube, Instagram ve diğer yüzlerce platformdan birine yüklediğinizde ise o açıklayıcı konum verileri de orijinal dosya ile birlikte varlığını sürdürmeye devam eder.

Aralık 2009'da CNBC'den Maria Bartiromo, Google'ın CEO'su Eric Schmidt'i programına konuk etmişti. Konuğuna, Google'ın kullanıcılarını artan şekilde takip etmesi sonucunda ortaya çıkan gizlilik endişelerini sorduğunda, Schmidt de uzun yıllar hatırlanacak bir cevap verdi: *"Başkalarının bilmesini istemediğiniz bir şeyiniz varsa belki de hiç yapmamanız gerekir."*

Schmidt ve diğerleri yanlış bir şey yapmadığınız sürece başka insanların (şirketlerin, hükumetlerin, belki de komşularınızın) ne yaptığınızı bilmesinden korkmamanız gerektiğini söylüyor. İçinde yaşadığımız bu yeni veri gözetim toplumunda *"Ama benim saklayacak bir şeyim yok ki!"* savunması kabul edilebilir görünmemektedir. Bu ifade, seçimlerimizi tamamen yanlış iki farklı yola sokuyor: Ya bütünüyle gözetilmeyi kabul ediyoruz ya da şüphelenilen suçlular kategorisine giriyoruz. Hepimizin hayatında bütünüyle kendine özel olması gereken anlar olabilir. Tek istisna, özgürce bu anları paylaşacağımız kişileri seçmek olabilmelidir. Bilgisayar güvenlik uzmanı Moxie Marlinspike'nin dediği gibi: *"Muhtemelen saklayacak bir şeyiniz var, sadece ne olduğunu bilmiyorsunuz."*

Dünyamızın her yanını saran dijital kirliliğe hep birlikte neden oluyoruz. Nasıl ki 20. yüzyılda kimse endüstriyel atıkları nehire boşaltma konusunda bir şey düşünmüyor ve sokağa çöp atmayı normal buluyorduysa biz de bugünkü dijital faaliyetlerimizin uzun vadede karşımıza çıkarabileceği sonuçları şimdiden algılayamıyoruz. *"Ben zaten hiçbir çevrim içi sosyal ağa katılmadım."* diyerek içinizi rahatlatmanız ise ne yazık ki mümkün değil. Arkadaşlarınız

fotoğraflarında sizi etiketleyecek, arabanızdaki GPS her an konumunuzu takip edecek ve kredi ya da banka kartınız tüm alışverişlerinizin listesini tutacak.

NSA ve CIA'da görev yapmış olan bilgisayar mühendisi Edward Snowden bir keresinde şöyle demişti: *"Gizleyecek bir şeyiniz olmadığı için mahremiyet hakkını umursamadığınızı iddia etmek, söyleyecek bir şeyiniz olmadığı için özgür konuşmayı umursamadığınızı söylemekten farksızdır."*

Teknoloji Dost mu Düşman mı?

Platon, retoriğin karşısında olan biriydi. Retoriği, *insanları kandırma sanatı* olarak ifade ediyordu. Platon'un öğrencisi Aristo'ya göre retorik, *ikna etmenin sanatıydı*. İyi niyetli de olunabilir kötü niyetli de. Sorun retorikte değil bu bilgilerin kimin eline geçtiğinde ve bu bilgilerle neler yaptığında. Bir hekimi düşünelim. Bu doktor yıllarca aldığı eğitim ve deneyimler sonucunda ulaştığı bilgi ve beceriyle insan sağlığının yararına da hizmet edebilir; aksi yönde bir organ mafyasında da görev alabilir. Teknoloji de bir araçtır. Yarar-zarar dengesi kişinin kullanım amacına göre değişir.

Teknoloji ile kullanıcılar arasına set çekmek yerine doğru ve bilinçli bir kullanımı önceliklenmelidir. Nitekim söz konusu bilgisayar sistemleri bugün uzayı keşfederken de ülkemizi savunurken de eğitim öğretim faaliyetlerini geliştirirken de finansal anlamda güçlenirken de yararlandığımız, çağımızın en yararlı araçlarından biridir.

Değerli Veliler,

Dijital teknolojiler, özellikle eğitim konusunda dezavantajlı durumda olan çocuklar için fırsatlar sunabilmektedir. Kullanıcısı olarak İnternet'in sunduğu fırsatlar kadar risk ve tehlikelerin de farkında olarak çevrim içi olabilmelidir.

Dijital teknolojiler ve İnternet hayatın bir parçası konumundadır. Şu aşamada odak noktası nasıl daha fazla yararlanılabileceği ve nasıl daha az zarar görülebileceği üzerine olmalıdır. Siber dünyanın yararları ve zararları onu kullanan kişinin niyeti ölçüsündedir. Bir örnekle İnternet teknolojileri uzakları yakın ederken yakınları da uzaklaştırabilmektedir. Nitekim bir araç olarak İnternet, kullanıcısı olan insanın doğasıyla uyum içerisinde hareket eder.

Ergenlik döneminin bir çıktısı olarak birey, kendi kişiliğini oluşturmaya ve erginliğe gidişte özünü tanımaya ve tanımlamaya

yönelik bir süreç içerisinde olur. Son çocukluk ve ilk gençlik yılları olarak literatürde tanımlanan bu dönemdeki kişi, bireyselliğini ve özgürlüğünü ispatlamak ister. Bu ispat çabası ise çoğunlukla aile içi çatışmaların ve uzaklaşmaların yaşanmasına yol açabilir. Bu uzaklaşma, dijitalde yeni bir kimlik oluşumuna itebileceği gibi gerek dış dünyada gerek sanal dünyada birtakım olumsuz durumların yaşanmasına da zemin hazırlayabilmektedir. Tam da bu noktada ebeveynlerin dikkati ve hassasiyeti önem arz etmekte, anlayış içerisinde konuya yaklaşmaları gerekmektedir. Nitekim çocuk, ebeveynlerinden sevgi ve saygı göremezse bu ihtiyacını dışarıda bir yerlerde gidermek isteyecektir. Bu da istenmeyen davranışların ve kalıcı olabilecek zararların ortaya çıkmasına neden olacaktır.

Olumsuz yönleri başlık olarak şöyle sıralanabilir:

- Teknoloji Bağımlılığı
- Dijital Ayak İzi
- Dolandırıcılık
- Bilginin Çarpıtılması
- Kara Propaganda
- Siber Zorbalık
- İstismar
- Kişisel Mahremiyetin İhlali
- Oltalama Saldırıları (SMS, E-posta…)

Bireysel ve toplumsal açıdan konuya yaklaşıldığında teknolojinin yüksek bir avantaj sağladığı da göz ardı edilmemelidir.

Olumlu yönleri başlık olarak şöyle sıralanabilir:

- Ulusal Güvenlik
- Eğitim ve Öğretimde Eşitlik ve Ulaşılabilirlik
- Sağlık Çözümleri
- İletişim Kolaylığı
- Sınırları Aşma Olanağı
- Ticari Faaliyet
- Kariyer Gelişimi

Siber Zorbalık

Siber zorbalık, İnternet ve sosyal medya platformları gibi dijital iletişim araçlarının bireyleri veya grupları taciz etmek, korkutmak veya zarar vermek için kasıtlı olarak kullanılması anlamına gelir. Siber zorbalığı yapan kişi, İnternet'te, yapısal olarak anonimliğin arkasına saklanabilmektedir. Zorbalığın dijital dünyadaki varlığı bu yönüyle yaygın görülen bir duruma dönüşmektedir. Nitekim her ne kadar kimliği gizlemek mümkün görünse de adli bilişim yöntemleriyle siber zorbalığı yapan kişinin bulunması ve adalet karşısında cezai yaptırımla karşı karşıya gelebildiğini de anımsatmakta yarar var.

Unutulmamalıdır ki *ortam sanal olsa da işlenen suç gerçektir* ve dışarıda, fiziki dünyada yapılan olumsuz davranışlarda olduğu gibi ceza yaptırımı uygulanır.

Siber zorbalığın sonuçları ciddi ve geniş kapsamlı olabilir. Mağdurlar duygusal sıkıntı, kaygı, depresyon ve akademik performansta düşüş yaşayabilir. Dahası, siber zorbalığa maruz kalan kişilerde kendine zarar verme veya intihara yönelim görülebilmektedir. Dijital iletişimin yaygın doğası, siber zorbalığın her an ortaya çıkabileceği ve geniş bir kitleye ulaşarak mağdur üzerindeki etkisini artırabileceği anlamına gelmektedir.

Siber zorbalık tehdit mesajları göndermek, söylentiler yaymak, utanç verici veya kişisel bilgileri paylaşmak, başkalarını taklit etmek veya küçük düşürmek için sahte profiller oluşturmak gibi çeşitli şekillerde ortaya çıkabilir. İlkokul ve ortaokul öğrencilerinde şakalaşma, eğlenme adı altında siber zorbalık normalleştirilebilmektedir.

Siber zorbalığı ele alma ve önleme çabaları, çeşitli paydaşları içeren çok yönlü bir yaklaşım gerektirmektedir. Eğitim kurumları, ebeveynler ve çevrim içi platform sağlayıcıları farkındalığın artırılması, dijital okuryazarlığın teşvik edilmesi ve etkili politika ile

kılavuzların uygulanmasında önemli roller oynamaktadır. Ebeveynleri olarak sizler, çocuklarınızla çevrim içi güvenlik hakkında aktif olarak açık konuşmalar yapmalı ve uygun İnternet kullanımı konusunda onlara rehberlik sağlamalısınız.

Siber zorbalık bireylerden, topluluklardan ve bir bütün olarak toplumdan dikkat ve eylem bekleyen ciddi bir konudur. Güvenli ve kapsayıcı bir çevrim içi ortamı teşvik ederek dijital okuryazarlığı destekleyerek ve etkili önleyici tedbirler uygulayarak siber zorbalığın zararlı etkilerini azaltmaya ve herkes için daha sağlıklı bir dijital ortam sağlanmalıdır.

İnternet, ceplere girmeden önce, okulda tatsız bir durum yaşandığında bu durum okulla, sınırlı sayıda kişiyle kalıyordu. Bu açıdan müdahale ve kontrol mekanizmaları ile mağdurları korumak daha kolaydı. Şu anda ise saatler içinde tüm sosyal paylaşım platformlarında binlerce kişinin bildiği bir duruma dönüşebilmekte; dahası yalan yanlış, eksik, art niyetli paylaşımlarla kontrolden çıkabilmekte ve bu mekandan bağımsızlık zamandan da bağımsız bir halde 7-24 sürebilen bir akışa yol açabilmektedir.

Sık Görülen Siber Zorbalık Türleri

1. Asılsız söylentiler yaymak, hedeflenen kişi hakkında dedikodular yapmak.
2. Dış görünümüyle alay etmek, uygunsuz takma adlar yakıştırmak.
3. Fiziksel baskıyı dijital ortama taşıyarak aşağılayıcı davranışlarda bulunmak.
4. Sosyal medyada, zorbalığa maruz kalacak kişinin adına sahte hesaplar oluşturarak o yapıyormuş gibi art niyetli paylaşımlar yapmak.
5. Kişinin bilgisi ve izni olmaksızın ona ait fotoğraf veya videosunu çekmek, herhangi birine göndermek ya da herhangi bir yerde paylaşmak; küçük düşürücü ya utandırıcı bir görüntüyle şantaj uygulayarak istemediği şeyler yapmaya zorlamak.

6. Sosyal medya platformlarından, oluşturulan okul veya topluluk gibi gruplardan kişiyi dışlamak.
7. Kişiyi dijital anlamda takip etmek ve ısrarla, istenmeyen biçimde taciz düzeyinde rahatsız etmek.
8. Anonim bir kimliğe bürünerek kişiye yönelik cinsel içerikte yazılar yazmak ya da görüntüler göndermek.
9. Hedeflenen kişinin dijital platformlardaki hesapların yaptığı paylaşımların altında yorumlar yazarak rencide etmek.
10. Zararlı yazılım içeren, virüslü bağlantılar ya da e-postalar göndermek.

Siber Zorbalığa Maruz Kalındığında Ne Yapmak Gerekir?

Siber zorbalığa maruz kalan çocuk ve gençlerin çoğu, yaşadıkları mağduriyeti kimseyle paylaşmadıkları, kendi başlarına çözmeye çalıştıkları ya da sessiz kalmak zorunda oldukları bilinmektedir.

Çocuğunuz fiziki ortamda olduğu gibi dijitalde de bir zorbalığa maruz kaldığında benzer tepkiler gözlemlenir. Davranış ve duygu durumları gözlenerek olası belirtiler takip edilmelidir. Çocuğunuz:

- Okula gitmek istemiyorsa,
- Telefonuyla geçirdiği zamanlarda gelen bir mesajla tedirginliği daha da artıyorsa,
- Uyuyamıyor, halsiz düşüyor ve öfkeleniyorsa,
- Sosyal çevresinden git gide uzaklaşıyorsa ve
- Okul içi ve okul dışı faaliyetlerindeki başarısında beklenmedik düşüşler varsa siber zorbalığa maruz kaldığına yönelik bir durumdan söz edilebilir.

Peki, böylesi bir siber suça ya da siber zorbalığa maruz kalındığında ne yapmak gerekir?

- Siber zorbalığın ölçüsü ve son durumu hakkında çocukla hoş görülü biçimde etkin bir iletişimde olunmalıdır. İçinde bulunduğu durum ruh sağlığında ciddi ve kalıcı zararlar

bırakabilir. Yaşananlarda onu suçlu olarak görmediğinizi, bu durumu birlikte aşabileceğinizi sözlü ve davranışsal olarak hissettirin.

- Öfkeyle karşı tarafa yönelik bir misilleme yapılmamalıdır. Bu sizi ve çocuğunuzu suça ortak yapar, haklıyken haksız duruma düşersiniz. Bunun yerine çocuğunuzla birlikte ortak hareket edin. Nitekim yaşanan olaylar sonucunda gururu kırılmış, özgüveni hasar almış bir durumda olacaktır. Olayların çözümünde dışarıda kalan bir mağdur değil çözümünde etkin yer alan bir konumda olması mental açıdan toparlanmasına da yardımcı olacaktır. Bununla birlikte bir sorunun üstesinden gelmenin, zorluklarla baş edebilmesine olanak tanımak için de güzel bir fırsat olarak görülmelidir.
- Karşıdaki şahıs hemen engellenmeli, asla muhatap olunmamalı, yanıt verilmemelidir. Zorbalık yapan kişi yanıt aldıkça kendini güçlü hisseder. Tersi durumda kontrol ona verilmiş olunur ve zorbalığın dozu git gide artar.
- Duruma göz yumulmamalı, çocuğunuz ya da bir tanıdığınız suça ya da zorbalığa maruz kalıyorsa sessiz kalınmamalıdır.
- Çocuğunuz güven hissiyle öğretmenine ya da ailesine konuyu açabilmelidir. Korkan çocuk, bir zorbalığa maruz kaldıysa kızacağınızı düşünerek bunu sizinle paylaşmayabilir. Koşulsuz sevgi ve saygıyla ona kucak açacağınızı hissedebilmesi önemlidir.
- Kanıtlar toplanmalı, asla silinmemelidir. Mümkün olduğu ölçüde ekran kaydı alınmalı, bir başka telefon ile video da çekilmelidir.
- Kanıtlarla birlikte savcılığa/emniyete/jandarmaya başvurmalıdır. Dijitalde ise gerekli bildirimler siber@egm.gov.tr adresine yapılabileceği gibi *112 Acil* hattı üzerinden de ihbarda bulunulabilir.

Kendinizi Nasıl Korursunuz?

Teknolojinin kendini güncellemesi ve zaman algısı bilinen çerçevenin dışında pek çevik ilerler. Bu devinim içerisinde teknolojiyi gündelik hayatın bir parçası olarak yararlarını öncelemek adına ister çocuk olsun ister yetişkin, teknolojiye getirilecek her türlü yasağın çözümden uzak olduğunun bilinmesi gerekir. Önceliğin genelleştirilmiş olarak kısıtlamalar ve yasaklar yerine bilinçli ve güvenilir ele alınması bireysel ve toplumsal gelişim için başat bir unsurdur. Aile içindeki iletişimin gücü oranında teknolojinin ev içindeki konumu belirleyici olmaktadır. Bunlarla birlikte anımsanmalıdır ki risk ve tehditler yalnızca çocuk ve gençleri değil yetişkin bireyleri de kapsamaktadır. Bu itibarla güvenlik önlemleri, teknolojiyi kullanan herkesin sorumluluk alanı içerisinde yer alır.

Dijital dünyanın olası risk ve tehditlerine karşı daha güvenli bir deneyim için önerileri şöylece sıralamak mümkündür:

1. Her şeyden önce çocuk öğüdü alırken kulaklarını kapatır, gözlerini açar. Annenin Instagram'da sürekli reels izlediği, babanın televizyon karşısından hiç kalkmadığı bir evde çocuktan kitap okumasını, ders çalışmasını beklemek pek işe yaramayacaktır. Bu durumda çocuk da oyun oynamayı tercih edebilir. Unutulmamalıdır ki anne-baba çocuk için ilk rol modeldir. Dünyadaki en çok güvendiği iki insan ne diyorsa ne yapıyorsa mutlak bir doğruluk içerisindedir onun için. Belli bir yaşa kadar bunun böyle olunduğu tecrübe edilmektedir.

2. Ortak bir alanda kullanılan cihazda giriş yapılacaksa "beni hatırla" kutusu işaretlenmemelidir. Giriş yapılan tüm platformlardan işiniz bitince pencereyi kapatmadan önce çıkış yapmayı unutmayınız. Özellikle toplu kullanım alanları olan İnternet kafe gibi yerlerde giriş yapılmaması önemlidir.

3. Dijital cihazlarınızın tümünde güvenlik duvarı etkin olmalıdır. Yanı sıra anti virüs yüklenmelidir.

4. Yazılım, uygulama ve sistem güncellemeleri mutlaka yapılmalıdır. Nitekim -çoğunlukla- her güncellemede bir güvenlik açığı giderilmiş olur.

5. Okul, iş yeri, toplu taşıma, kütüphane, İnternet kafe gibi ortak kullanım alanlarında parola gerektiren yerlere giriş yapılmamasına özen gösterilmelidir. Mecbur kalındıysa ve başka da bir seçenek yoksa çıkış yapılması unutulmamalı ve eve dönüldüğünde (güvenli bir İnternet ağı üzerinden) parola hemen güncellenmelidir. Bu gibi durumlar için geçici bir e-posta açılabilir.

6. Kredi/banka kartı bilgileri alışveriş sitelerine kayıtlı olarak tutulmamalıdır.

7. APK dosyaları yalnızca kendi platformundan edinilmelidir. Dış kaynaktan bir uygulama indirip kurduğunuzda davetsiz misafirleri de cihazınıza buyur etmiş olursunuz. Google Play ve App Store gibi resmi marketlerde bile yararlı görünen fakat zararlı faaliyet yürüten uygulamalar olabilir.

8. Herkese açık (ortak ağlar: kafe, havalimanı, meydan, toplu taşıma vs.) WiFi ağlarına bağlanılmamalıdır. Çok gerekliyse kendi telefon ağınızı (hotspot / mobil veri) açınız ve bilgisayarınızı bağlayınız.

9. ATM'de, markette, kafede ve POS'la işlem yapılan her yerde parola girerken tuşlar elle gizlenmelidir. Mümkünse temassız ödemeye geçilebilir.

10. WiFi parolası dışarıdan biriyle paylaşılmamalıdır. Komşuyla ortak İnternet kullanımı olabilir ya da eve gelen misafir, ağa bağlanmak isteyebilir. Bu durumda, o kişilerin yapacağı olumsuz bir durumda ağ sizin olduğu için kendinizi karakolda ifade verirken bulabilirsiniz.

11. WiFi bilgileri varsayılan olarak tutulmamalı; adı ve parolası değiştirilmelidir. Varsayılan parolaları hacklemek daha kolaydır ve bir önceki durumdaki gibi yasa dışı bir iş yapılırsa sizin ağınız üzerinden geçen tüm eylemlerden tüm sorumluluk sizin olur.

12. İlkokul ve ortaokula giden çocuğunuz için TRT Çocuk ve Emniyet Genel Müdürlüğü iş birliğinde yapılan "Ekip: SİBERAY" çizgi filmini öneririz. Dijital dünya, yazılım ve güvenlikle ilgili üç arkadaşın macerasını 12 dakikalık 14 bölümde anlatmaktadır. YouTube'tan da izlenebilmektedir.

13. Telefona kurulan uygulamanın cihazda nelere erişim izni istediğine dikkat edilmelidir. Örneğin bir "Günlük Planlayıcı" sizin kişi listenize, kameranıza, mikrofonunuza, SMS okumasına-yazmasına yönelik erişim iznini neden talep ediyor olsun? Yine de o uygulamayı yüklemek kaçınılmaz ise -en azından- uygulama kullanılırken erişmek istediği özelliğe erişebilmesine müsaade edilmeli, arka planda sürekli erişimine izin verilmemelidir.

14. Bilgisayar, tablet ve telefonlarda belli aralıklarda fotoğraf, video ve yazışmalar gözden geçirilmelidir. Aynı oranda kullanılmayan yazılım ve mobil uygulamaların temizliği de gözden kaçmamalıdır. Çocuğunuz, bilmediği bir kaynaktan yazılım ya da mobil uygulama yükleyebilir. Belli aralıklarla cihazda neler yüklü olduğu denetlenmeli, uygulamanın cihazda nerelere erişebildiğine dikkat edilmelidir.

15. Toplu taşımada, kafede ve kütüphanede olduğu gibi kapalı alanlarda veya yürürken tüm ortak alanlarda omuz sörfü ile cihazınız gözetlenebilir. Parola ile giriş yapılacaksa daha dikkatli olunmalıdır. Özel ve hassas içerikli bir belge, yazı, görsel ve tüm içerikler bunu göz ardı etmeyerek açılmalı ya da açılmamalıdır. Omuz sörfünü yapan bir insan olabileceği gibi güvenlik kameraları da bu kapsamda gözetleyici bir konumda yer alabilir.

16. İnternet'e yükleyeceğiniz bir bilgiyi (bu, işiniz için bir doküman da olabilir, kardeşinizin mezuniyet fotoğrafı da olabilir) yükle/paylaş butonuna basmadan önce şunu kendinize sorun: *Bu bilginin yarın burada olmasının bir sakıncası olur mu?* Bir gönderiyi İnternet'e yüklemek için paylaş butonuna çoğu zaman gerek yoktur; JavaScript burada devreye girerek siz daha klavyeden tuşladığınız anda o bilgiyi veri tabanına kaydedebilmektedir. Vazgeç/iptal gibi butonların orada olması da "güvenilir liman" hissiyatı vermekten başka bir şey değildir. Ana fikrimizi burada anımsatmakta yarar var: *Siber uzay, dışarıdaki yaşamdan daha güvenli değildir.*

17. Olabildiğince az *akıllanalım* ve şunu soralım: Bu teknolojiye gerçekten ihtiyacım var mı? Olmasa da olur mu?

Çocuğunuzu Nasıl Korursunuz?

Bu ifadeler tanıdık geliyor mu?

> *"Bugünlerde gençler kontrolden çıkmış durumda. Kaba bir şekilde yemek yiyorlar. Yetişkinlere karşı saygısızlar. Anne-babalarına karşı çıkıyorlar ve öğretmenlerini sinirlendiriyorlar."*[2]

> *"Günümüzün gençleri öyle umursamaz ki ileride ülke yönetimini ele alacaklarını düşündükçe umutsuzluğa kapılıyorum. Bizlere, büyüklere karşı saygılı olmayı, ağırbaşlı davranmayı öğretmişlerdi. Şimdiki gençler kurallara boş veriyorlar. Çok duyarsızlar ve beklemesini bilmiyorlar."*[3]

> *"Bu gençlik nereye gidiyor?"*[4]

Her dönemin kendi içinde dünyayı algılayışında birtakım farklılıklar söz konusu olabilir. Yukarıdaki ifadelerde de görüldüğü üzere beş bin yıl öncesinde dahi yetişkinlerin gençlere yönelik beklentilerinin karşılanmayışına yönelik serzenişleri okumak mümkün olabiliyor. Geçmişe yönelik özlemin bir çıktısı olarak da değerlendirilebilecek bu tepkinin haklılığını tartışmaktan öte Aristo'ya, Heseoid'e ve Sümer tabletine ait olarak alıntılanan yukarıdaki ifadeleri sırayla eklemekte amacımızın, günümüzün çocuklarını ve gençlerini anlamaya yönelik bir anımsatma olarak değerlendirilmelidir.

Konu güvenlik olunca tat kaçıran konuları olabildiğince şeffaf biçimde ele almak gerekmektedir. Bu konuları konuşmayı gündeme almak bile bazen rahatsız edici olabilir. Psikolojik olarak bilinmeyenin verdiği belirsizliklere karşı kendinizi, ailenizi ve

[2] Aristo, M.Ö. 335.
[3] Heseiod, M.Ö. 800.
[4] Sümer tableti, M.Ö. 3000.

çocuklarınızı korumanın yolu karşı karşıya kalınan durum hakkında bilgi edinmek ve onu tanımaktan geçer.

Sanal dünya -fiziki dünyada olduğu üzere- dışarıda bir yerlerde iyi ve kötü insanların olabildiği gibi dijital dünyada da bu durum böyledir. Dahası, teknolojik imkanlar doğrultusunda kötü niyetli paylaşımların ve kişilerin daha güçlü olabildiğini söylemek de mümkündür. İnternet'te her içerik doğru olmadığı gibi her kişi de gerçekten kendisi olmayabilir. Sorgulayıcı bir bakış açısı kazanması açısından bu konuları doğrudan çocuğunuzla konuşunuz. Onun güvenliği ve esenliği adına nasıl ki çocuğunuzu gerçek hayattaki olası tehlikelere karşı uyarıyor ve bu noktada kurallar koyuyorsanız sanalda da benzer bir tutum sergilemelisiniz.

Kötü niyetli kişiler, dijital ortamda istismar edeceği kişinin güvenini kazanmak adına farklı kimlik takınarak arkadaşlık kurabilmektedirler. Süreç içerisinde konu ve içerik taciz boyutuna evrilebilmekte ve bu yönde çocuktan taleplerde bulunulabilmektedir. Bu aşamadan önce çocuğun istenmeyen görüntüler vermesi durumunda karşı taraf bunu bir şantaj olarak kullanmakta ve zamanla dozu artan istekleri çocuğa dayatabilmektedir. Bu durum karşısında korkan çocuk durumu ailesine bildirmekten çekinebilir çünkü bu durumda ele geçirdiği fotoğraf ve videoları ifşa etmekle tehdit ediliyor olabilir. Kontrolü ele geçirdiğinin farkında olan saldırgan, sanal buluşmaların yerini fiziki buluşmalara kadar taşıyabilir. Bu noktada ebeveynleri olarak sizler çocuğunuzla etkin ve hoşgörülü bir iletişim kurabilmelisiniz. Ortada bir hata varsa -suçlayıcı bir tavırdan sakınarak- önceliğiniz bu durumu çözüme kavuşturmak ve çocuğunuzu güven altına almak olmalıdır.

Dijital cihazların fiziki korunmasına da dikkat edilmelidir. Bir kafede, toplantıda, kütüphanede, toplu taşımada… Olası bir kayıp ya da çalıntı durumunda telefon, tablet ve bilgisayar gibi kişisel verilerin bulunduğu bu cihazlar kötü niyetli kişilerin eline geçebilir. Her ne kadar kırılma olasılığı olsa da kayıp ya da çalıntıya karşı güçlü parolalarla cihazların korunması yapılmalıdır. Teknolojik

cihazlarınızın bir başkasının eline geçebileceğini düşünerek içerisindeki kişisel ve mahrem verilerin tutulmasına dikkat edilmelidir.

Kişisel verilerinizi paylaşırken…

Şimdinin bebekleri, bütünüyle dijital bir çevrenin içerisinde doğuyorlar. İşte böylesi bir çevrede doğan ve bir parçası gibi teknolojiden yararlanabilen çocuk için siber güvenlik farkındalığı kazandırmak ilk günden önceliğe alınmalıdır. Yaşının küçük olması, konunun önemini azaltmadığı gibi çocuğun erken yaşlardaki savunmasızlığına istinaden daha da artmasına zemin bırakmaktadır. Buradan hareketle çocuğunuzun yaşı ne olursa olsun kullandığı teknolojik cihazlarla ilgili güvenlik algısının sizler tarafından ele alınması, yaptığı ve yapacağı tüm hareketlerin bir sonucu olabileceği, risk ve tehditlerle karşılaşabileceği, karşılaştığında ise nasıl bir tutum sergilemesi gerektiğini özümsemesi gerekmektedir.

Bebek, henüz doğmadan önce bile doğum anına ait fotoğraf ve video kayıtlarının dahi sosyal medyada yer aldığı bir yaygın kullanım alışkanlığı söz konusudur. Bütünüyle "iyi niyetli" olarak bu paylaşımları yapan aileler sevinçlerini dostlarıyla paylaşırken çocuğa yönelik ilk dijital ayak izlerini de böylelikle oluşturmaya başlamış oluyorlar. Ailenize yeni bir üye katıldığında, gözünüzden sakındığınız çocuğunuzu (sosyal medyada da) başkalarından da sakının. Onun bilgisi ve rızası olmadan yapılan her paylaşımda kişisel verilerini ifşa etmiş olabileceğinizi göz ardı etmeyin.

Çocuğunuzla (ve kendinizle, ailenizle) ilgili yapacağınız bir paylaşımda şu sorular belirleyici olabilir:

1. Bu paylaşımda yer alan fotoğraf, video ve içeriğe dair tüm bilgiler yarın bir gün çocuğumun aleyhinde önüne çıkabilir mi?

2. Çocuğum, bu paylaşım nedeniyle mahcup duruma düşebilir mi? Bu paylaşım onu utandırabilir mi?
3. Çocuğumun kişiliği hakkında nitelikli bilgileri dostlarımızın dışında başkalarının da erişebilmesine karşı korun(a)madığı bir ortamda, ailem hakkında özel paylaşımlar yapmaya bu kadar istekli olmalı mıyım?
4. Kötü niyetli kişilerin bu paylaşımdaki içeriklere erişimi söz konusu olduğunda bundan rahatsız olur muyum? Ben olmaz isem paylaşımda yer alan diğer kişilerin söz hakkını onlar adına vermem etik olur mu?
5. Peki, gerçekten de bunu paylaşmalı mıyım? Çok net olarak: *Buna gerek var mı?* Başkalarının bunları bilmesinde ne gibi bir kazanımım olacak? Etkileşim ve yapay beğeniler alabilmek adına kişisel verilerimi açığa çıkarmaya değer mi?

Dijital teknolojilerin içinde doğan çocuk, henüz okuma yazma dahi bilmeden teknolojik cihazları anne ve babasından daha iyi kullanabildiği örnekler çoktur. Bununla birlikte denilmelidir ki teknolojiyi kullanabilmenin onun güvenli kullanıldığı anlamı çıkmamalıdır. Nitekim akıllı telefonlar ve tabletler, özünde kolaylıkla kullanılabilmesi önceliklenerek tasarlanmaktadır. Pratikte kullanılan cihaz üzerinde hakim bir görüntü çizilse de yapıları gereği çocuklar, sanal dünyanın risklerine yetişkinlerden daha açıklardır çünkü bu denli yoğun bir kullanım içerisinde olmak olası risk ve tehditleri fark edemez hale getirebilmekte, kişiyi rehavete düşürebilmektedir.

Yönetemediğimiz sistem güvenli değildir yaklaşımı doğrultusunda ebeveynleri olarak sizlerin de en az çocuklarınız kadar teknolojiyi kullanabiliyor olmanız gerekir. Peki, bu konu neden bu denli önemli? Örneğin, hesap makinesi işlevi olarak görünen ve açıldığında bir hesap makinesi gibi çalışan “Calculator Vault” gibi bir “çözüm”den habersizseniz, çocuğunuz, galerisinde yer alan fotoğraf ve videoları ya da her neyi saklamak istiyorsa bunları sizden gizleyebilir.

Çocuğunuz teknolojiyle tanıştığında onun yanında olabilmeniz, denetimli bir gözlemle olası risk ve tehditlere karşı bağışıklığının güçlenmesinde en güvendiği kişiler olarak yanında olmanız gerek fizikselde gerek sanalda kendine olan öz güvenine de olumlu katkılar sağlayacaktır. Ebeveyn-çocuk ilişkisinin sağlıklı ve sürdürülebilirliği açısından iletişim kanalının açık ve hoşgörülü olduğunu bilmesinde yarar var. Böylece olası bir sakıncalı durumu size açıkça bildirebilir.

Çocukluk ve ergenlik dönemlerindeki arkadaşlığın bir göstergesi olarak (bir tür ispatlama) kişisel verilerin paylaşımı, parolaların karşılıklı ya da karşılıksız verilmesi gibi durumlar yaşanabilmektedir. Bu noktada atalar sözüne kulak asmalı: *Sırrını düşmanın bilmesin dersen dosta dahi açma*. Şirazlı Sadi de bu konuda bize şöyle seslenir: *Sırlarını en yakın, en has adamlarına bile söyleme*. Unutulmamalı ki o özel dostların da çok özel dostları vardır. Tecrübelerle sabittir ki dostluk, her zaman devam etmeyebilir.

Çocuğunuzun bilgisayar, saat, tablet ya da telefonla dijital dünyayla ilk temasından itibaren kullanım ve güvenlikle ilgili temel bilgileri anlatmak ve uygulamalı göstermek gerekir. Fiziki dünyada onun güvenliği için aldığınız önlemlerde olduğu gibi dijital dünyada da aynı hassasiyeti gösterdiğinizi hissetmesinde yarar var. Çocuğunuz, dışarıda markete giderken ya da okuldan dönerken kullandığı toplu taşımada ona öğrettiğiniz güvenlik kurallarını bildiği gibi sanal dünyada da zaman geçirirken benzer kuralları sizden duymalı, uygulayıp uygulanmadığına yönelik yine sizin denetiminizin olduğunu bilmeli.

Öncelikli amacımız çocukları teknolojiden uzak tutmak değil olası risk ve tehditlere karşı onları sakınmak; dahası, bunu süreç içerisinde kendi başlarına yapabilecek biçimde donatabilmek olmalıdır.

Yukarıdaki perspektif doğrultusunda daha güvenli bir dijital dünya ve güvenilir siber kullanıcı olmaları, teknolojinin güçlü yanlarını

kullanabilen bir birey olmaları noktasında çocuklarınız için alabileceğiniz önlemleri şöylece sıralamak mümkündür:

1. Dışarıdan hiç kimse çocuğunuzu sizin kadar iyi tanıyamaz. Konu güvenlik ve mahremiyet olduğunda, bu hassasiyeti gözeterek her koşulda onun yanında olmayı ihmal etmeyiniz.

2. Çocuğunuzun odasında tek başına kalabileceği (oyun konsolu, bilgisayar, tablet, telefon…) teknolojik cihaz olmamalı. Unutmayınız ki orada -çevrim içi dünyada- tek başına değil. Fiziksel dünyada yanından dahi geçmesini istemeyeceğiniz kişiler dijital dünyada her an yanındadır. Fiziki dünyada camdan bakardınız, çocuk kiminle ne oynuyor görürdünüz. Sanal dünyada ise potansiyel olarak çevrim içi olan 6 milyar insanla karşılaşma durumu söz konusudur.

3. Bilgisayarın ortak bir yerde olması ve monitörün sizlerin de görebileceği biçimde konumlandırılmasında fayda görülmektedir. Eve bilgisayar alınacaksa dizüstü yerine masaüstü tercih edilmelidir. Nitekim taşınabilir bilgisayarın (ya da tabletin) hareketliliği dolayısıyla çocuğunuzun nerelerde ve neyle zaman geçirdiğini bilemeyebilirsiniz ve böylece şeffaflık ortadan kalkmış olur. Sürekli peşinde olmanız durumunda ise aile içi çatışmaların yaşanması da pek olasıdır.

4. Çocuğunuzun izlediği müzik klibine, diziye, filme ve animeye, okuduğu kitaba, oynadığı oyuna siz de ortak olun. Çocuğunuzu tanımak ve dijital dünyada neler yaptığını anlayabilmek adına onun kullandığı uygulamaları kullanın, oynadığı oyunları oynayın. Böylece olası yararlar ve zararları doğrudan gözlemleyebilirsiniz.

5. Banka girişinde, sosyal medyada ve olanak tanınan her yerde iki faktörlü doğrulamayı etkinleştiriniz.

6. Mümkün olduğu ölçüde üyelik oluşturduğu yerlerde kendi fotoğrafı yerine avatar kullanmasını öneriniz.

7. Çocuğunuza telefon vermek durumundaysanız hat operatörlerinin bütünü İnternet'e çıkış için belli kısıtlamaları yapabilmektedirler. İlgili mağazaya gidip ya da çevrim içi olarak "Güvenli İnternet" tercihlerinizi ayarlayabilirsiniz. Operatör tarafından sunulan ücretsiz bir servistir. Bu yöntem genç bireyler için pek işe yaramayabilir çünkü VPN ile Türkiye'den girişi yasaklı siteler dahi açılabilmektedir. Genellikle ilkokul öğrencileri için geçerli bir yöntem olarak görülebilir. Yine de anımsanmalıdır ki *yasaklar tatlıdır*. Ayrı bir başlıkta bu konu üzerinde duracağız.

8. Bilgisayar-tablet-telefon gibi cihazlarda denetim için saat aralığı, uygulama bazında kullanım süresi kısıtlaması mümkündür. Android cihazlar için "Google Family Link" uygulaması tercih edilebilir. iOS cihazlarda varsayılan ayarlar aracılığıyla benzer çözüm söz konusudur. Bu yöntemi tercih edecekseniz çocuğunuzla iş birliği içerisinde yürütmeniz sürekliliği sağlayacaktır. Uygulamalara erişim ve kullanım süresinin kısıtlamasını ortak bir zeminde belirlerseniz sağlıklı bir anlaşma olacaktır. Neden bu kotanın konulduğunu anlarsa sınırları aşmak için farklı yolları denemek istemeyebilir. Nitekim bu sınırları aşmak pek kolaydır.

9. Çocuk olgunlaştıkça, sanal dünyanın olumsuz yanlarını görebilecek duruma geldikçe otokontrol ona teslim edilmelidir. Nitekim, hayatın her alanında onun yanında olamayacağınız gibi sanal dünyada da bir başına güvenli hareket edebilmeyi öğrenmesi gerekmektedir. Böylece çocuğun sorumluluk duygusunun ve bilincinin de gelişmesine olanak tanınmış olur. Bunlarla birlikte unutulmamalıdır ki küçük yaşlardaki çocukların dünyayı algılamadaki yaklaşımları, onları savunmasız kılmaktadır.

10. Çocuğunuz okul öncesi bir dönemde ise izin verdiğiniz ölçüde oynaması, izlemesi, okuması, dinlemesi gereken içerikleri indirip telefonu-tableti öyle verebilirsiniz. İnternet bağlantısı olmaksızın çevrim dışı ve bütünüyle sizin denetiminizde bir çözüm olabilir. Dahası "uçak modu" etkinleştirilerek dış dünyadan gelebilecek tüm sinyalleri kapalı tutabilirsiniz. Böylece enerji ihtiyacı da azalacaktır.

11. Çocuğunuzun gelişimine katkı sağlayabilecek siteleri, hesapları, sayfaları bulup bunları takip etmesini önerebilirsiniz.

12. TikTok ve Snapchat, özellikle küçük yaştaki kız çocukları için sanal dünyadaki en tehlikeli yerler arasında. Uygulama adı fark etmeksizin benzer platformlara karşı daha dikkatli olunmalıdır.

13. Banyoya ve tuvalete telefon götürme alışkanlığı da son dönemlerin yaygın bir davranışı olarak görülmektedir. Telefonu/tableti belli bir konumda sabitleyip dizi izleyerek, şarkı dinleyerek duş alındığı bilinmektedir. Banyo, tuvalet ve yatak odaları gibi kişisel mahremiyetin olduğu yerlerde teknolojik cihazların yer almasındaki sakıncalar açıktır.

14. Son yıllarda yaygınlaşan "akıllı çocuk saatleri"nde yer alan dahili mikrofon, kamera ve GPS gibi modüllerin mahremiyete yönelik çeşitli zafiyetler barındırdığı bilinmektedir. Bazı çözümlerin ciddi güvenlik ve mahremiyet sorunları doğurduğunu bilmeli, yeni bir teknolojiyi hayata katarken gerçekten gerekli olup olmadığı tartışılmalıdır.

15. Parolalar diş fırçası gibidir. Birkaç ayda bir değiştirmeli, güçlendirmelidir. Tüm hesaplarda aynı parola kullanmamalıdır. Doğum tarihi, plaka, aileden birinin adı, memleket gibi açık bilgiler seçilmemelidir.

16. Kullanılmadığında bilgisayarın, tabletin ve cep telefonunun ön ve arka kameralarına bant çekerek kötü niyetli kişilerin uygulamalar aracılığıyla izniniz dışındaki erişimlerini önleyebilirsiniz.

17. Kimden geldiğini bilmediğiniz/emin olamadığınız e-postaları, ek dosyalarını açmayınız.

18. Telefona yüklenilen uygulamaların istediği izinler hususunda daha dikkatli olunmalıdır. Not tutma uygulamasının konumunuza, kişi listenize, SMS'lerinize ya da mikrofonunuza ulaşmak istemesi normal değildir.

19. Güvenli olmayan sitelerden alışveriş yapmamalı, kredi kartı bilgilerinizi kaydetmeyiniz. URL adresinde sitelerin *http* değil *https* ile başlamasına dikkat ediniz.

20. Sosyal medya hesaplarında tanımadığı kişilerden gelen arkadaşlık isteklerini kabul etmemeli ve onları eklememelidir. Tanıdığı bir kişi olarak sahte bir hesap açılabileceğini de bilmelidir. Bu gibi durumlarda çocuğunuz, o kişinin gerçekten o olup olmadığını nasıl teyit edebileceğini bilmelidir.

Peki, bireyin mahremiyeti ne olacak? Bu kadar denetim, bu kadar gözetim, bu kadar her şeyine karışmak kişisel alanına girmek demek değil midir? Haklısınız. Fiziki olgunluk, mental olgunluk gibi dijital olgunluk da artık gündemimizde yer alması gereken bir kavramdır. Çocuğunuz belli bir dijital olgunluğa erişene değin bu denetimli kullanım alışkanlıkları sürdürülmelidir. Olgunluğun doğrudan yaşla bir ilgisi olmadığına göre onu en iyi tanıyabilecek durumda olan siz ebeveynlerin kararı başat olacaktır.

Değerli Veliler,

Sanal dünya, fiziksel hayatımızdan daha güvenli değildir.

Çocuğunuz, dijital dünyada yaptığı her olumsuz hareketin bir suça dönüşebileceğini de bilmelidir. Fiziksel dünyada olduğu gibi sanal dünyada da tehlikelerin varlığını küçümsememelidir.

Yasaklar Tatlıdır

Teknolojinin yapısı dolayısıyla herhangi bir kısıtlama olası görünmemektedir. Küçük yaştaki çocuklar için belli ölçülerde bu mümkün olsa da teknoloji okuryazarlığı ilerleyen çocuk ve gençler için bu yöntemler zayıf kalmaktadır. Tüm bunlara ek olarak anımsanmalıdır ki aşırılık, karşıtını doğurur ve süreç içerisinde onu besler. Buradan hareketle yaklaşımımız yasaklayıcı bir tutumdan öte çocukla iş birliği içerisinde olarak onun bilgisi dahilinde süreci yönetmek olmalıdır. Otokontrolü sağlayacak dijital olgunluğa erişene değin bir denetimin onun güvenliği için yapıldığını bilmesi öz güveni açısından da büyük önem taşır. Hatırda tutulmalıdır ki gelişimsel olarak çocuklar ve ilk gençlik dönemindeki ergenlerin dijitalde kurdukları bağlantıların ve karşılaştıkları içeriklerin güvenilirliğini gözden geçirecek bir eleştirel bakış açısına sahip olmaları genelde olası değildir.

Çocuğa yönelik konulan kısıtlamaların nedenini gerekçeleriyle ve anlaşılır biçimde anlatılması ve atılan adımların gerekçesi anlaşılabilir olduğu takdirde davranışların yönetilebilmesi ve çizilen sınırlar içerisinde kalınabilmesi daha kabul edilebilir olabilir. Çocukların yasaklara karşı gelme, yasaklananı sergilemeye yönelik eğilimleri yüksektir. Yanı sıra anlamlı bir çerçeve çizilemediği durumda söz konusu kısıtlamalar bir biçimde aşılabileceği gibi çocuğunuz üzerinde sözünüzün etki gücünde de azalma riski ortaya çıkacaktır.

İnsan hayatının varlığı başat unsuru olan su bile fazla içildiğinde zarar verebilir. Atalar sözünde olduğu üzere *azı karar çoğu zarar* bilinciyle

ilerlenmelidir. Dijital ortamda gereğinden fazla tüketilen zamanı verimli etkinliklere yönlendirebilmek gerekir.

Katı sınırlamalar getirmek ve yalnızca olumsuz yönlerine odaklanmak yerine teknolojiye yönelik açık ve ilgi çekici bir yaklaşımı teşvik etmenin, farkındalığı ve yönergelere bağlılığı teşvik etmede daha etkilidir. Çocuğunuzun dünyasını anlayabilmek adına ilgi gösterdiği oyunları oynamak, sosyal medya platformunda hesap açmak, takip ettiği diziyi/animeyi izlemek gibi dijital deneyimlerine aktif olarak katılarak çocuklarınızla çevrim içi dünyaları hakkında sohbetler başlatabilirsiniz. Böylece -varsa- olumsuz yönlerini görmelerini sağlayabilirsiniz.

Ona rağmen değil onun için önlemler aldığınızı onun da hissetmesini sağlamanız gerekir. Onun haklarının ve ihtiyaçlarının gözetildiği geliştireceğiniz ve uygulayacağınız dijital politikanızın merkezinde onun ve ailenizin olduğunu bilmesi, dahası, birlikte bir politika tasarlanmasıyla birlikte söz konusu içeriğe birlikte uyum sağlanma olasılığı artacak ve böylece benimsenebilecektir. Nitekim onların hayatını etkileyecek olan bir kararda çocuklarınıza da söz hakkı vermek güçlü bir kişilik oluşumuna da doğrudan katkı sağlayacaktır.

Çocuğun ekran başında ne kadar kalması gerektiği ise aile içindeki dinamiklere ve çocuğun ihtiyacına göre değişiklik göstermektedir. Bu kararı çocuğunuzla birlikte verirken dijitalde ne kadar zaman geçirdiğinden de önemlisi bu süreç içerisinde ne yapılacağı da göz önüne alınmalıdır.

İnternet'in yapısı gereği bir hizmetin önüne geçilmesi, kısıtlanması, engellenmesi olası değildir. Buradan hareketle çocuğun güvenliği ve mahremiyeti için atılacak adımlar ve uygulanacak yöntemlerde çocukla iş birliği içerisinde olunmalı ve birlikte hareket edilmelidir. Hazır bulunuşluk ve dijital olgunluk düzeyinde ise otokontrolü kendisine bırakmak kişisel gelişimi için de uygun bir davranış olacaktır.

Teknolojiyi kısıtlayan değil olası risklerinden korumak öncelik olmalı, dahası, teknolojiyi yalnızca tüketen değil üreten tarafta yer alınması adına özendirici tutum sergilenmelidir. Kişisel mahremiyet bilincinde olan çocuk kendini koruyabileceği gibi bir başkasının sınırlarına da saygılı bir davranışı benimsemeyi refleks haline getirebilir.

İnternet'te bir şeyin yasaklanması teoride ve pratikte mümkün olsa da aşılabilirliğinin kolaylığından dolayı işlevsel değildir. Zaten evde ve bireyselde ne kadar yasaklarsanız yasaklayın evden çıktığında servise/toplu taşımaya binecek, okula gidecek ve orada sizin kontrolünüzden uzak bir biçimde olacak arkadaşlarıyla (arkadaşlarının dünyasından parçalarla) öğrenecek ki buna literatürde *örtük* ve *gizil öğrenme* denir.

Ergenlik döneminde beyin, karar verme ve duygusal düzenlemeyi etkileyen önemli değişiklikler geçirir. Mantıklı düşünme ve dürtülerin denetiminden sorumlu olan *prefrontal korteks* tam olarak gelişmemişken duygulardan sorumlu olan *amigdala* oldukça etkin bir durumdadır. Bu noktada ergenler, akranları tarafından kabul görmek için riskli davranışlarda bulunabilirler. Soyut düşünme yetenekleri muazzam ölçüde gelişmiş olsa da temel mantıkla mücadele edebilir ve duygularını yönetmekte zorlanabilirler. Ergenlere anlayış ve destekleyici bir üslupla yaklaşmak önemlidir çünkü geleneksel anlamda tavsiye veya ceza yöntemleri gelişimin bu aşamasında etkili olmayabileceği gibi size karşı bir tutum içerisine de onları itebilir.

Peki, teknolojinin aşırı kullanımına karşı alınan bu kadar denetim ve kısıtlama yapıldıktan sonra çocuk ne yapacak? Elbette "elinden alınan"ın yerine koyulacak değerli etkinlikler gerekir. Alternatifler neler olacak? Çocuğunuzla bunu konuşarak -onun yerine karar vermeden- bir liste çıkarmak yerinde olabilir. Belki yeni bir kurs… Belediyenin düzenlediği ve yüz yüze gidebileceği mahalledeki kültürel, teknik ya da sportif bir kurs. Kişisel finans yönetimi, zihinsel ve bedensel dinçlik, sanat ve teknik beceriler, iletişim…

Değerli Anne ve Babalar,

Bir çocuk için anne ve babanın yerini ne bir arkadaş ne bir öğretmen doldurabilir. Onların gözünde gerçek bir kahraman olarak sizlerin davranışları örnek bir model olarak karşılarında durmaktadır.

Biliyoruz ki yaşları her ne olursa olsun onlar sizin için hep çocuk kalacaklar. Bir ömür boyunca, hangi koşulda ve ne durumda olursa olsun gözünüzden sakındığınız çocuklarınıza kılavuzluk etmek, onları hayatın güçlüklerine karşı hazırlamak ve olası tehlikelerden korumak içgüdüsel olarak varlığın ayrılmaz bir parçasıdır.

Teknolojinin gelişimi ve dönüşümünün bu denli hızlı yaşanması ise siz ebeveynleri hiç olmadığı kadar çağa uygun davranışları ve yetkinlikleri edinmeye çağırmaktadır.

Son Söz

Turan ÇİNKILIÇ
Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi
Okul Müdürü

———

Sayın Anne ve Babalar,

Literatür incelendiğinde ele alınan çalışmaların ağırlıklı olarak dijital bağımlılık ve zorbalık üzerine yoğunlaştığı görülmektedir. Tüm bu kıymetli çalışmalarda gözlemlenen bir eksiklik ise işin siber güvenlik tarafıydı. *"Ebeveynler için Siber Güvenlik"* kitabımızla birlikte bu ihtiyacı karşılamış olmaktan dolayı kıvançlıyız.

Öğretmenliğimin yanı sıra bir baba olarak şunu diyebilirim ki dijital dünyanın faydaları olduğu kadar zararları da vardır ve burada biz ebeveynlere ciddi iş düşmektedir. Çocuklarımıza gereken özeni bizler göstermezsek bunu kendi çıkarları uğruna yapmaya heveslilerin az olmadığını dostane hatırlatmak isterim.

Siber güvenlik lisesi olarak çocuklarımıza yönelik sorumluluğumuzun bilinciyle Siber Vatan'ımız için çalışmalarımızı güçlendirerek artıracak gerek akademik yayınları gerek teknik projeleri öğretmen-öğrenci iş birliğinde hayata geçireceğiz.

Türkiye Cumhuriyeti Devleti'nin 100. yılını kutladığımız ve yeni yüzyılına girdiğimiz bu dönemde Başöğretmenimiz Atatürk olmak üzere Anadolu'yu bizlere ebedi yurt yapan aziz şehitlerimizi saygıyla anıyorum. Bıraktıkları emaneti daha nice yüzyıllara taşımak için, güçlü mesleki ve teknik eğitimde var gücümüzle çalışmaya, üretmeye devam edeceğiz. Bu çalışmanın ortaya çıkmasında katkı ve katılım sağlayan hocalarıma teşekkürü bir borç bilirim.

İstanbul, 26 Ocak 2024

TEKNOPARK
İSTANBUL
Mesleki ve Teknik
ANADOLU LİSESİ

Ebeveynler için Siber Güvenlik

Dijital Dünyada Kendinizi ve Çocuğunuzu Nasıl Güvende Tutarsınız?

ISBN 978-625-6736-73-3

www.teknoparkistanbul.meb.k12.tr