1. İnternetin Kullanım Alanları ve Sağladığı Faydalar

İnternet teknolojilerinin gelişmesi insanların birbiriyle olan iletişimini kolaylaştırırken, birçok yenilikleri de beraberinde getirmiştir. İnternet, haberleşmeden bilgi paylaşımına, habercilikten medyaya, tanıtım ve reklamdan seyahat ve tatile, kamu hizmetlerinden bankacılık ve ticarete, eğlenceden sosyal ilişkiler ve kültürler arası etkileşime, çevre ve sağlıktan eğitime ve günlük yaşamı ilgilendiren pek çok alanda olumlu getiriler ve yenilikleri hayatımıza getirmiştir.

İnternet birçok bilgiye rahatlıkla ulaşabilme, insanları duygu ve düşüncelerini rahatlıkla ifade edebilme ve dijital platformda oluşturduğu sosyal arkadaşlıklar ile iletişim kurma olanağı sağlamıştır. İnternetin sağladığı fırsatları ana başlıklarla şöyle sıralamak mümkündür (Güler, 2016):

- Güncel Haber ve Bilgi Sağlama: İnternetin dünyada en büyük etkisi, bilgiye ve habere anında ulaşma imkânı sunmasıdır. Öyle ki, İnternet sayesinde dünyanın en ücra köşesinde dahi gelişmelerden anlık haberdar olmak mümkündür. Hatta herkesin bir muhabir gibi gelişmeleri paylaşma imkânı bulunmaktadır.

- Görüş ve Bilgi Paylaşma: İnternetin önemli özelliklerinden birisi, kişinin herhangi bir olay ya da kişiye dair görüşünü aktarabileceği platformlara sahip olmasıdır. Blog, web sayfası ya da sosyal ağ hesabı gibi araçlarla kişinin kendi hakkında bilgi paylaşma ya da görüş bildirme imkânı bulunmaktadır.

- Zaman ve Mekândan Bağımsız, Eş zamanlı ve Eş Zamansız İletişim Sağlama: İnternet, kişiler arasında çoklu ve interaktif iletişim imkânı getirmiştir. İletişimin ucuz ve hızlı olması, insanların sosyal hayatlarını yeniden biçimlendirmelerini gerektirmiştir.

- Ekonomik ve Hızlı Haberleşmeye Olanak Sağlama: İnternetin özellikle endüstriyel alanda getirdiği önemli bir avantaj, maliyeti çoğu kez sıfırlayan haberleşme yöntemidir. Hayatın ekonomiyle ilgili her alanında bu hız ve maliyet düşüşü kendini

göstermiş, ekonomik hayatın merkezine de internetin oturduğu görülmüştür.

- Görsel ve İşitsel Öğelerle İletişim Kalitesini Artırma: İnternetin getirdiği iletişim ve paylaşım imkânı, görsel ya da görüntülü unsurları da barındırmaktadır. Bu özellik, ilişkilerin, alışverişin, çalışma hayatının hatta eğitimin içeriğinin de yeniden şekillenmesi sonucunu doğurmuştur.

2. İnternetle Gelen Sorunlar

İnternet birçok alanda insan hayatını kolaylaştırması ile birlikte teknolojik alanda en büyük yeniliklerden birini sağlaması, aynı zamanda birçok risk ve tehdittin de zaman içerisinde doğmasına sebep olmuştur. İnternetin yaygınlaşması ve kullanımının oldukça kolaylaşması aynı zamanda bu platformun zaman içerisinde istismarına ve kötü amaçlı kullanımlarına da sebep vermiştir.

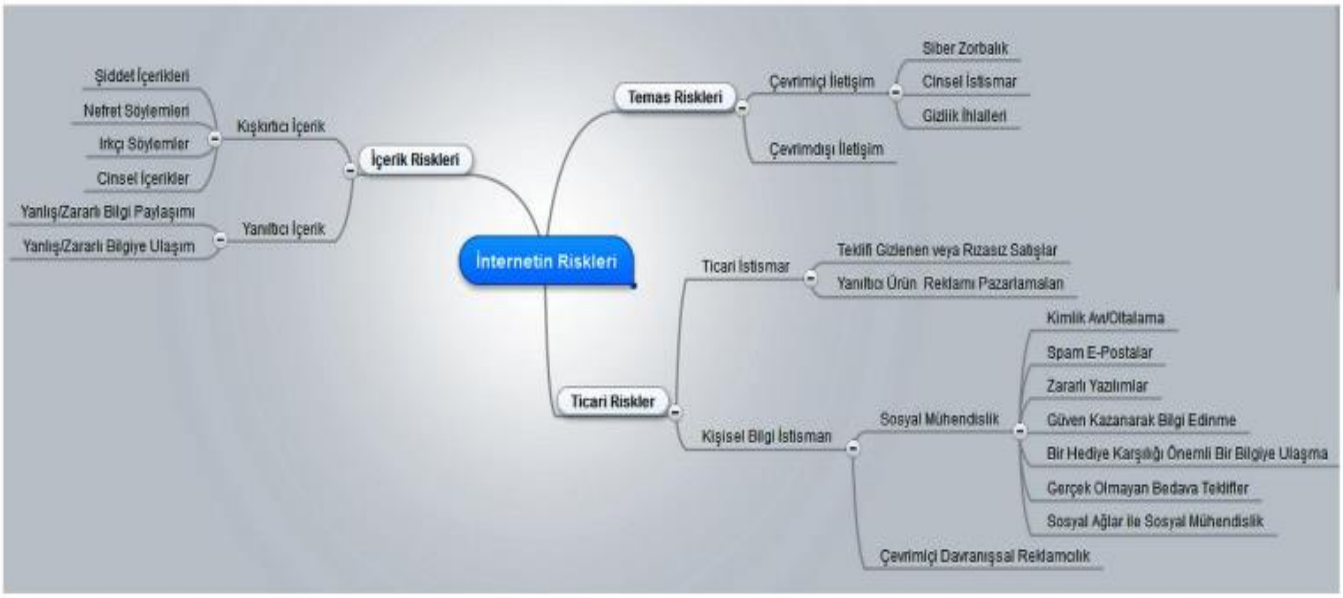
İnternetin riskleri sınıflandırılmalarında şimdiye kadar yapılmış en kapsamlı sınıflandırmalardan bir tanesi de De Moor ve arkadaşlarının yapmış olduğu çalışmadır. De Moor ve arkadaşları internetin risklerini Şekil-1'de de görüldüğü üzere 3 temel başlık altında inceleyip içerik, temas ve ticari riskler olmak üzere belirlemişlerdir (Valcke, Bonte , De Wever , & Rots , 2010). Bu çalışma kapsamında, De Moor ve arkadaşlarının belirlemiş olduğu 3 risk sınıflandırmasının alt başlıkları Çubukcu ve Bayzan tarafından farklı açılardan bakılarak aşağıdaki gibi incelenmiştir (Çubukcu & Bayzan, 2013).

2.1. İçerik Riskleri

İnternet içerik riskleri, web sitelerinin barındırdığı görsel ve yazılı negatif içeriklerdir. Bu içerikler farklı şekillerde internet kullanıcılarını olumsuz olarak etkileyebilmektedir. Kışkırtıcı şiddet söylemleri ve görselleri, nefret söylemleri ve görselleri, ırkçı söylemler ve görseller, cinsellikle ilgili içerikler, içeriğin derecesine göre kullanıcılar üzerinde olumsuz etkiler bırakabilmektedir. Bununla birlikte doğru olmayan yanlış ve zararlı bilgiler de, bu bilgilere

ulaşan her internet kullanıcısı için ayrı bir risk oluşturmakta ve internette bilgi kirliliğine sebep olmaktadır. Bu tür doğru olmayan bilgiler büyük bir risk oluşturmakla birlikte, internet kullanıcılarının da doğru bilgiye ulaşmasını zorlu ve karmaşık hale gelmesine sebep olmaktadır (Çubukcu & Bayzan, 2013).

Şekil 1 – İnternetin Riskleri



2.2. Temas Riskleri

Temas riskleri, çevrimiçi ve çevrimdışı iletişimde riskler olmak üzere incelenmektedir. Çevrimiçi iletişim, siber zorbalık, çocukların cinsel istismarı ve gizlilik ihlalleri olmak üzere sınıflandırılmakla beraber tüm bu risklerin çevrimiçi ortamda özellikle çocukların tanımadığı insanlarla iletişime geçerek ve istismarcıların kendilerini olduğundan farklı göstererek (‘grooming’: kötü niyetli irtibat) çocuklarla iletişime geçmesi sonucu ortaya çıkmaktadır. Çevrimiçi bu temasın gerçek hayatta yüz yüze buluşma noktasına taşınması ise çevrimdışı iletişim olarak adlandırılmaktadır.

Siber zorbalık, bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme, kaba davranma ve kötü söz söyleme davranışlarının tümü olarak tanımlanmaktadır. Olayın daha çok teknik yönünü içeren elektronik zorbalık (electronic bullying) ve diğeri ise olayın daha çok psikolojik yönünü içeren elektronik iletişim (e-iletişim) zorbalığı (e-communication bullying) olmak üzer iki çeşit zorbalıktan bahsedilebilir (Arıcak, 2011).

Cinsel istismar, bir kişinin kendi rızası dışında cinsellik içeren bir eyleme maruz kalmasıdır. Eğer bu eylem internet üzerinden yapılıyor ise çevrimiçi (online) cinsel istismar olarak adlandırılmaktadır. Cinsel istismar, söz ile yapılabileceği gibi eyleme dönüştürülerek şiddet ve zorlama şeklinde de gerçekleştirilebilir. İnternet ortamında çevrimiçi iletişimle başlayıp, çevrimdışı buluşmayla noktalanan internet arkadaşlıkları cinsel istismarlara neden olabilmektedir. Çevrimiçi cinsel istismarın en büyük nedeni, internet ortamında kendini farklı kişilik ve yaş gruplarında gösteren yabancı kişilerle bilinçsiz bir şekilde sonucunu düşünmeden kurulan arkadaşlıklardır.

Gizlilik ihlalleri, internetin anonim yapısı gerekliliği sonucu ortaya çıkan ihlalleri oluşturmaktadır (Valcke, Bonte , De Wever , & Rots , 2010). Ev adresi, kimlik numarası, telefon numarası, anne kızlık soyadı, aile bireylerinin adı ve diğer kişisel bilgilerin internet ortamında doğrudan veya dolaylı olarak paylaşılması sonucunda da gizlilik ihlalleri çok rahatlıkla kendine ortam bulabilmektedir (Çubukcu & Bayzan, 2013).

2.3. Ticari Riskler

Ticari risklerin en büyük ayağını dijital vatandaşların kişisel verilerinin istismar edilmesi sonucu kimlik avı/oltalama (phishing) ve benzeri yöntemlerle dolandırılması vakaları oluşturmaktadır. Tüm bunları sosyal mühendislik veya kimlik hırsızlığı başlığı altında toplayabiliriz.

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen dolandırıcılık yöntemidir. Kredi kartı ve internet bankacılığı bilgileri, şifre ve

parolalar, elektronik posta ve diğer önemli kişisel bilgilerin bir başkası tarafından çıkar sağlamak amacıyla kullanıldığı bir dolandırıcılık türüdür. Kimlik hırsızlığında kullanılan en önemli yöntemlerin başında oltalama(Phishing) ve zararlı (casus) yazılımlar (keylogger, spyware) gelmektedir. Oltalama, dolandırıcıların banka, kredi kartı bilgilerini güncellemek amacıyla sahte e-posta göndererek kişileri sahte web sitesine yönlendirerek kişisel bilgilerin girilmesi sağlanarak ele geçirilmesi gibi yöntemleri kapsamaktadır. Gönderilen e-postanın gerçek kuruluştan geldiğini göstermek için kuruluşa ait logo, gerçek web sayfasının birebir kopyası ve diğer sahte bilgiler kullanılabilmektedir. Diğer bir yöntemde zararlı yazılım içeren siteler yoluyla kişilerin bilgisayarlarına keylogger, truva atı ve diğer casus yazılımları yüklemek için zararlı programların kullanıcının dikkatini çekmek için isminin değiştirilip bilgisayar indirilmesi sağlanarak yapılmaktadır.

Diğer zararlı (casus) yazılımlar ise tanıtım, kişisel bilgi toplama veya kullanıcıların onayı almadan bilgisayarın yapılandırmasını değiştirme gibi belirli davranışları gerçekleştiren yazılımlar için kullanılan genel bir terimdir. Casus yazılımlar, genellikle başka bir program kurulurken, kullanıcının da onayı ile bilgisayara kurulan ve kurulduktan sonra kişinin internetteki gezme alışkanlıkları ilgili bilgi toplayan ve bu bilgileri internet üzerinden kötü niyetli kişilere iletebilen yazılımlardır.

Bunların dışında internet üzerinden yapılan gerçekliği olmayan bedava veya gerçekçi olmayan ticari teklifler de kullanıcıları farklı web sitelerine yönlendirmek suretiyle kişisel bilgileri elde etme amacı gütmektedir. İstenmeyen e-postaları (spam) da bu kategoride değerlendirmek gerekir. Bu tür e-postalarda kullanıcının hiçbir talebi olmadan e-posta adresine gönderilmiş zararlı ekler veya yazılımlar içeren e-postalardır. Bu e-postaların açılması kişisel bilgilerin bu e-postayı gönderenlerin eline geçmesine de aracılık edebilmektedir.

Sosyal mühendislik yöntemleri kullanıcıları kandırıp, mali kazanç sağlama amacıyla sıklıkla kullanılabilmektedir. Bunların dışında, dolandırıcılık amacı gütmeyip kullanıcılara teklifi gizlenmiş bir şekilde rızasız satışlar gerçekleştirebilme veya yanıltıcı ürün katalogları ile

reklam ve pazarlama stratejileri izleme suretiyle de dijital vatandaşlar ticari risklerle karşı karşıya kalabilmektedir.

Her ne kadar bir risk unsuru olup olmadığı tartışmalı bir konu olsa da Çevrimiçi Davranışsal Reklamcılık (ÇDR) son zamanların popüler konu başlıklarından birini oluşturmakta ve bu konuda farklı görüşler ortaya konulabilmektedir. ÇDR, dijital vatandaşların ziyaret ettikleri web sitelerinin sınıflandırılması ve kişisel iletişimlerinin analizi sonucu vatandaşlara da çoğu zaman izlendiklerinin haberi doğrudan veya dolaylı yönden verilmeden internet ortamında vatandaşa özel ilgi alanlarına göre reklam ve pazarlama içeriklerinin sunulması yöntemidir. ÇDR uygulamaları asıl olarak kullanıcının bilgisayarına sunucular tarafından bırakılan çerezler (cookie) vasıtasıyla yürütülmekle birlikte birçok ÇDR uygulaması tarayıcıların kendi çerezlerini değil, flash programının çerezlerini de kullanılabilmektedir (Kırlıdoğ, 2013). 2002/58/EC sayılı Avrupa Birliği Direktifi ve bu Direktifi izleyen diğer çalışmalar ile web sitelerinin kişisel bilgileri toplaması ve çerez kullanımı ile bilgilendirme koyma zorunluluğu getirilmesine rağmen bunun uygulanabilirliği sektörde tam işlememektedir (Çubukcu & Bayzan, 2013).

KAYNAKLAR

Arıcak, O. T. (2011). *Siber Zorbalık: Gençlerimizi Bekleyen Yeni Tehlike*. 5 15, 2013 tarihinde Kariyer Penceresi: http://www.kariyerpenceresi.com/?yazarlarimiz,51,104/siber-zorbalik-genclerimizi-bekleyen-yeni-tehlike-.html adresinden alındı

Çubukcu, A., & Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. Middle Eastern & African Journal of Educational Research, 5, 148-174.

Güler, N. (2016). İnternette Çocuklara Yönelik Riskler ve Ailelerin Bilinçlendirme Faaliyetlerindeki Rolü, Bilgi Teknolojileri ve İletişim Kurumu Henüz Yayınlanmamış Uzmanlık Tezi, Ankara.