



T.C. İÇİŞLERİ BAKANLIĞI
**SİVİL TOPLUMLA
İLİŞKİLER**
GENEL MÜDÜRLÜĞÜ



SİBER ZORBALIĞA KARŞI MEDYA ETİĞİ REHBERİ EL KİTABI

**ÇEVİRİMİÇİ TEHDİTLERE VE RİSKLERE KARŞI
KORUMA SAĞLAYIN.**

"Dijital Şiddet: Gençler Arasında Siber Zorbalığa Karşı Medyanın Sorumluluğu" projesi, T.C. İçişleri Bakanlığı, Sivil Toplumla İlişkiler Genel Müdürlüğü tarafından desteklenmektedir.

PROJE DESTEK VE YASAL UYARI BEYANI

*Bu yayın, T.C. İçişleri Bakanlığı Sivil Toplumla İlişkiler Genel Müdürlüğü tarafından desteklenen “**Dijital Şiddet: Gençler Arasında Siber Zorbalığa Karşı Medyanın Sorumluluğu**” projesi kapsamında basılmıştır.*

Yasal Uyarı: Bu kitapta yer alan tüm görüş, düşünce, bulgu ve değerlendirmeler tamamen İnternet Medya ve Bilişim Federasyonu’na ait olup, T.C. İçişleri Bakanlığı Sivil Toplumla İlişkiler Genel Müdürlüğü’nün resmî görüşünü ve politikasını yansıtmaz. Kitap içeriğinde yer alan bilgilerin doğruluğu, özgünlüğü ile doğabilecek her türlü hukuki, idari, mali ve akademik sorumluluk münhasıran yazarına aittir. Sivil Toplumla İlişkiler Genel Müdürlüğü bu çalışmanın içeriğinden ve olası sonuçlarından sorumlu tutulamaz.

Okuyucuya Not: *Bu kitabın yorumlanması ve kullanımı okuyucunun sorumluluğundadır.*





Dr. Süleyman BASA

İnternet Medya ve Bilişim Federasyonu (İMEF)
Genel Başkanı

Dijital çağ, bilgiye erişimi kolaylaştırırken aynı zamanda bireylerin güvenliği, mahremiyeti ve toplumsal huzuru açısından yeni sorumluluklar da doğurmuştur. Bugün internet ve sosyal medya; haberleşmenin, eğitimin, ticaretin ve iletişimin vazgeçilmez bir parçası haline gelirken, siber zorbalık, dezenformasyon, kişisel verilerin ihlali ve dijital itibarın zarar görmesi gibi önemli riskleri de beraberinde getirmektedir. Bu nedenle dijital dünyada etik değerlerin korunması, yalnızca bireysel bir tercih değil, toplumsal bir sorumluluktur.

Elinizde bulunan “Siber Zorbalığa Karşı Medya Etiği Rehberi”, dijital dünyanın sunduğu fırsatları doğru değerlendirebilmek ve karşılaşılabilecek risklere karşı bilinç oluşturabilmek amacıyla hazırlanmıştır. Rehberimiz; siber güvenlik, siber zorbalık, gizlilik ve mahremiyet, internette dezenformasyon ve yanlış bilgilendirme, dijital ayak izi, dijital kimlik ve dijital itibar gibi günümüzün en önemli konularını medya etiği perspektifiyle ele almaktadır.

İnternet, doğru kullanıldığında insanlığın ortak bilgi hazinesidir; yanlış kullanıldığında ise bireylerin haklarını ihlal eden, toplumsal güveni zedeleyen ve geleceğimizi olumsuz etkileyen bir araca dönüşebilmektedir. Özellikle çocuklarımızın ve gençlerimizin dijital ortamlarda güvenli şekilde var olabilmeleri, medya okuryazarlığı becerilerinin geliştirilmesi ve etik ilkelerin benimsenmesi büyük önem taşımaktadır.

Bu süreçte medya kuruluşlarına, gazetecilere, eğitimcilere, ailelere, kamu kurumlarına ve sivil toplum kuruluşlarına önemli görevler düşmektedir.

İnternet Medya ve Bilişim Federasyonu olarak dijital dönüşümün merkezinde insanı esas alan, hak ve sorumluluk dengesini gözeten, etik değerleri önceleyen bir medya anlayışını savunuyoruz. İnanıyoruz ki güçlü bir dijital toplum; yalnızca teknolojik altyapıyla değil, bilinçli kullanıcılar, etik yayıncılık anlayışı ve güvenilir bilgi ekosistemiyle inşa edilebilir. Siber zorbalığa karşı mücadele etmek, yanlış bilgiyle etkin şekilde mücadele etmek ve dijital mahremiyeti korumak, hepimizin ortak görevidir.

Bu rehberin; öğrencilerimize, ailelerimize, eğitimcilerimize, gazetecilerimize, kamu kurumlarımıza ve dijital dünyada yer alan tüm bireylere yol gösterici bir kaynak olmasını temenni ediyor, daha güvenli, daha etik ve daha bilinçli bir dijital gelecek için önemli bir katkı sunacağına inanıyorum.

Bu çalışmanın hazırlanmasına destek veren İçişleri Bakanlığı, Sivil Toplumla İlişkiler Genel Müdürlüğü'ne, projeye katkı sağlayan tüm akademisyenlere, uzmanlara, eğitimcilerimize, sivil toplum kuruluşlarına ve emeği geçen herkese en içten teşekkürlerimi sunuyorum.

Dr. Süleyman BASA

İnternet Medya ve Bilişim Federasyonu (İMEF)
Genel Başkanı



Prof. Dr. Zakir AVŞAR

DİJİTAL ŞİDDET VE SİBER ZORBALIĞIN ÖNLENMESİNDE MEDYANIN ROLÜ VE ÖNEMİ

Bilgi ve iletişim teknolojilerindeki hızlı dönüşüm bireylerin sosyal etkileşim biçimlerini, kamusal alan anlayışını ve toplumsal ilişkilerin yapısını derinden etkilemiştir.

İnternet temelli iletişim ağlarının yaygınlaşması, sosyal medya platformlarının gündelik hayatın merkezine yerleşmesi ve mobil cihazların erişilebilirliğinin artması, iletişimin mekân ve zaman sınırlarını büyük ölçüde ortadan kaldırmıştır.

Bu dönüşüm bilgiye erişim, ifade özgürlüğü ve katılımcı iletişim açısından önemli fırsatlar sunarken, yeni risk alanlarının doğmasına da zemin hazırlamıştır.

Söz konusu risklerin başında dijital şiddet ve siber zorbalık gelmektedir.

Günümüzde dijital ortamlar, bireylerin kendilerini ifade ettikleri, sosyal bağ kurdukları ve kamusal tartışmalara katıldıkları alanlar olmanın ötesinde saldırganlık, manipülasyon, dışlama ve psikolojik baskı biçimlerinin üretildiği mecralar hâline de gelebilmektedir.

Dijital şiddet elektronik iletişim araçları aracılığıyla bireye zarar verme, psikolojik baskı

kurma, tehdit etme, aşağılama, sindirme ya da mahremiyetini ihlal etme amacı taşıyan davranışların bütünü ifade etmektedir.

Bu kavram, geleneksel şiddet biçimlerinden farklı olarak fiziksel temas gerektirmeyen; fakat bireyin psikolojik bütünlüğü, sosyal ilişkileri ve toplumsal konumu üzerinde son derece yıkıcı etkiler oluşturabilen bir olgudur.

Siber zorbalık ise dijital şiddetin en görünür ve en yaygın biçimlerinden biridir. Kasıtlı biçimde zarar verme amacı taşıyan, çoğunlukla süreklilik gösteren ve taraflar arasında güç dengesizliği barındıran çevrimiçi saldırgan davranışlar siber zorbalığın temel bileşenleri arasında yer almaktadır.

Hakaret içerikli mesajlar, çevrimiçi taciz, ifşa kültürü, kimlik taklidi, dedikodu yayma, itibarsızlaştırma girişimleri, tehdit içerikleri ve dijital dışlama bu davranışlara örnek teşkil etmektedir.

Siber zorbalığın geleneksel zorbalıktan ayrıldığı temel noktalardan biri, dijital ortamın sunduğu anonimlik ve sürekli erişilebilirlik imkânıdır.

Çevrimiçi platformlar saldırgan bireylere kimliklerini gizleme fırsatı sunarak cezai veya toplumsal yaptırımlardan kaçınma olanağı sağlayabilmektedir.

Bu durum, saldırgan davranışların daha kolay ortaya çıkmasına neden olmaktadır.

Bunun yanında dijital ortamın zamansız yapısı, mağdurun güvenli alan algısını da zedelemektedir.

Geleneksel zorbalık belirli mekânlarla sınırlı kalabilirken, siber zorbalık bireyin evinde, okulunda, iş yerinde ya da özel yaşamında kesintisiz biçimde etkisini sürdürebilmektedir. Böyle bir durum mağdurun sürekli tehdit altında hissetmesine ve yoğun psikolojik baskı yaşamasına yolaçmaktadır.

Araştırmalar siber zorbalığın özellikle çocuklar, ergenler, kadınlar, göçmenler, etnik azınlıklar ve kırılgan toplumsal gruplar üzerinde daha yıkıcı sonuçlar doğurduğunu göstermektedir.

Gelişimsel açıdan kimlik oluşum sürecinde bulunan genç bireyler çevrimiçi saldırılara karşı daha savunmasız bir konumda yer almaktadır. Bu saldırılar özgüven kaybı, akademik başarısızlık, sosyal izolasyon, kaygı bozuklukları, depresyon ve travmatik stres belirtilerine yolaçabilmektedir.

Daha ağır vakalarda intihar düşünceleri ve kendine zarar verme davranışlarıyla karşılaşılması meselenin ne kadar ciddi bir halk sağlığı sorunu olduğunu ortaya koymaktadır. Bu bağlamda siber zorbalık, bireysel bir iletişim problemi olarak değil sosyal politika, eğitim, psikoloji, hukuk ve medya çalışmaları ekseninde ele alınması gereken multidisipliner bir mesele olarak değerlendirilmelidir.

Dijital şiddetin önlenmesinde hukuki düzenlemeler, ebeveyn denetimi, eğitim politikaları

ve platform güvenlik sistemleri önemli unsurlar arasında yer alsada medya, bu mücadelede son derece stratejik bir konumda bulunmaktadır.

Medya, toplumsal bilinç oluşturma kapasitesi yüksek bir kurumdur. Kitle iletişim araçlarının kamuoyu üzerindeki etkisi, bireylerin belirli olayları nasıl algıladığını ve bu olaylara karşı nasıl tepki geliştirdiğini büyük ölçüde belirlemektedir.

Bu çerçevede medya, dijital şiddetin görünür kılınması, toplumsal farkındalığın artırılması ve koruyucu davranış kalıplarının geliştirilmesi bakımından kritik bir işlev üstlenmektedir.

Geleneksel medya araçları olan televizyon, radyo, gazete ve dergiler, geniş kitlelere ulaşabilme güçleri sayesinde siber zorbalık konusunda farkındalık oluşturma potansiyeline sahiptir.

Özellikle haber programları, uzman söyleşileri, kamu spotları, belgeseller ve eğitim temelli yayınlar aracılığıyla toplumun farklı kesimlerine dijital şiddetin boyutları aktarılabilir.

Medyanın burada üstleneceği rol, olayı sansasyonel biçimde sunmaktan ziyade neden-sonuç ilişkileri içinde analiz ederek toplumsal öğrenmeyi desteklemektir. Şiddetin dramatize edilmesi ya da tıklanma odaklı bir içerik ekonomisine dâhil edilmesi, mağduriyetin yeniden üretilmesine neden olabilmektedir. Bu sebeple etik habercilik anlayışı, dijital şiddetle mücadelede temel gerekliliklerden biri olarak öne çıkmaktadır.

Medya çalışmalarında önemli bir yere sahip olan gündem belirleme kuramı medyanın hangi konuları toplumsal tartışmanın merkezine taşıdığını açıklamaktadır. Bir konu medyada ne kadar görünür hâle gelirse, kamuoyu tarafından önemsenme düzeyi de o ölçüde artmaktadır.

Siber zorbalık meselesinin düzenli ve bilinçli biçimde medya gündeminde yer alması, toplumun bu sorunu ciddiyetle ele almasını kolaylaştırmaktadır. Bunun yanı sıra çerçeveleme kuramı da medyanın olayları hangi bağlam içinde sunduğunun toplumsal algıyı şekillendirdiğini göstermektedir.

Eğer medya siber zorbalığı basit bir "gençlik sorunu" veya "çevrimiçi tartışma" şeklinde sunarsa, meselenin psikolojik ve sosyal boyutları görünmez hâle gelebilir. Buna karşılık hak temelli ve mağdur merkezli bir sunum, sorunun gerçek etkilerini daha net ortaya koymaktadır.

Sosyal medya platformları, dijital şiddet tartışmalarında paradoksal bir konuma sahiptir. Bir taraftan siber zorbalığın en yoğun biçimde üretildiği alanlardan biri olarak dikkat çekerken, diğer taraftan toplumsal dayanışma ve dijital aktivizm için güçlü araçlar sunmaktadır.

Hashtag kampanyaları, farkındalık projeleri, psikolojik destek ağları ve dijital savunuculuk faaliyetleri sayesinde kullanıcılar kolektif bilinç geliştirebilmektedir.

Özellikle genç kuşakların medya tüketim alışkanlıkları göz önünde bulundurulduğunda, sosyal medya üzerinden yürütülen bilinçlendirme çalışmalarının etkisi oldukça yüksektir.

Medyanın siber zorbalıkla mücadelede üstlenmesi gereken bir başka önemli görev dijital okuryazarlığın geliştirilmesidir.

Dijital okuryazarlık, teknolojik araçları kullanabilme becerisinden çok daha kapsamlı bir kavramdır. Bu beceri çevrimiçi içerikleri eleştirel değerlendirme, dezenformasyonu ayırt etme, kişisel verileri koruma, güvenlik risklerini tanıma ve etik dijital davranış geliştirme kapasitesini kapsamaktadır.

Dijital okuryazarlığı yüksek bireyler, siber zorbalık davranışlarını daha erken fark edebilmekte ve uygun müdahale yollarını kullanabilmektedir. Medya destekli eğitim kampanyaları, bu becerilerin topluma yayılmasında önemli katkılar sunmaktadır.

Burada medya profesyonellerinin sorumluluğu da dikkatle ele alınmalıdır. Gazeteciler, editörler, yayıncılar ve dijital içerik üreticileri, haber üretim süreçlerinde etik ilkelere bağlı kalmakla yükümlüdür.

Mağdurun mahremiyetini korumak, travmatik deneyimleri istismar etmemek, şiddeti sıradanlaştırmamak ve nefret söyleminin dolaşımını engellemek bu sorumlulukların başında gelmektedir.

Etik ilkelere uzaklaşan yayın politikaları, dijital şiddeti azaltmak yerine derinleştirebilir. Bu nedenle medya etiği, siber zorbalıkla mücadelede teorik bir tartışma başlığı olmaktan çıkarak pratik bir gereklilik niteliği kazanmaktadır.

Dijital platform şirketlerinin algoritmik yapıları da bu bağlamda tartışılması gereken önemli bir boyut oluşturmaktadır. Etkileşim odaklı algoritmalar çoğu zaman öfke, çatışma ve kutuplaşma doğuran içerikleri daha görünür kılabilir.

Çünkü yüksek etkileşim alan içerikler platform ekonomisi açısından daha fazla trafik üretmektedir. Bu durum, dijital şiddetin yayılma hızını artırabilmektedir. Medya okuryazarlığı ile algoritmik farkındalık arasındaki ilişki bu noktada önem kazanmaktadır.

Kullanıcıların karşılaştıkları içeriklerin platform tasarımı tarafından nasıl şekillendirildiğini anlamaları, dijital şiddetin sistematik boyutunu kavrayabilmeleri açısından önem taşımaktadır.

Siber zorbalıkla mücadelede kalıcı başarı, devlet kurumları, eğitim sistemleri, sivil toplum kuruluşları, aileler, teknoloji şirketleri ve medya kuruluşlarının eşgüdümlü çabalarını gerektirmektedir.

Medya bu ekosistem içerisinde bilginin dolaşımını sağlayan, toplumsal duyarlılığı artıran ve davranış değişimini teşvik eden merkezi bir aktör konumundadır.

Güçlü bir medya stratejisi, bireylerin dijital haklarını tanımasına, çevrimiçi şiddete karşı bilinç geliştirmesine ve daha güvenli dijital topluluklar oluşturmaya katkı sunmaktadır.

Sonuç olarak dijital şiddet ve siber zorbalık, dijital çağın en karmaşık toplumsal sorunlarından biri olarak karşımıza çıkmaktadır.

Bu sorun, teknolojik gelişmenin sosyal etkilerini anlamayı zorunlu kılmaktadır. Medya, bu mücadelede pasif bir gözlemci değildir aksine toplumsal normları etkileyen, davranışları şekillendiren ve kolektif farkındalık inşa eden dönüştürücü bir güçtür.

Etik habercilik, bilinçlendirme faaliyetleri, dijital okuryazarlık çalışmaları ve hak temelli yayıncılık anlayışı, medyanın siber zorbalığın azaltılmasına sağlayabileceği katkının temelsütunlarını oluşturmaktadır.

Daha güvenli, daha adil ve daha kapsayıcı bir dijital kamusal alanın inşası, medyanın sorumluluk bilinciyle hareket etmesine güçlü biçimde bağlıdır.

Prof. Dr. Zakir AVŞAR





**GENÇLERE
İNTERNET GÜVENLİĞİ HAKKINDA
BİLGİ VERİN VE DİJİTAL
DÜNYALARINA DAHİL OLUN**

13 Siber
Güvenlik

25 Siber
Zorbalık

37 Gizlilik
Mahremiyet

48 İnternetteki Dezenformasyon
ve Yanlış Bilgilendirme

60 Dijital Ayak İzi, İtibar ve
Dijital Kimlik

A person wearing a dark hoodie is seen from behind, sitting at a desk and working on a laptop. The laptop screen is glowing with a bright blue light. The background is a dark blue space filled with numerous glowing blue padlocks of various sizes, some of which are connected by thin, glowing blue lines that resemble circuitry or data paths. The overall atmosphere is one of digital security and cyber defense.

Siber Güvenlik

Siber Güvenlik

Erken yaşlardan itibaren önleyici alışkanlıklar edinmek çok önemlidir. Kişisel güvenliğimizin cihazlarımızın güvenliğine bağlı olduğunu unutmamalıyız.

İNTERNET GÜVENLİĞİ NEDEN ÖNEMLİ?

Bağlantılı bir dünyada, hatalarımızdan veya kötü uygulamalarımızdan yararlanmaya çalışan art niyetlilerin erişim alanındayız.

Kötü amaçlı yazılımlar internette her yerde bulunur ve küçük rahatsızlıklardan ciddi kişisel sorunlara kadar her şeye neden olabilir, bağlı cihazlarımıza gizlice girebilir veya biz de istemeden kendimiz bulaştırabiliriz.

Siber suçlar ayrıca aldatmayı kullanır ve hassas bilgileri yanlış yerde vererek veya yanlış bilgileri gerçekmiş gibi kabul ederek hatalarımızdan yararlanmaya çalışır. Bazen de zayıf bir parola kullanmak, çalınmasını kolaylaştırır ve böylece başkaları cihazlarımızın ve uygulamalarımızın kontrolünü ele geçirebilir ve sonuç olarak dijital yaşamımızı ve bilgilerimizi de ele geçirebilir.

TEHLİKELER NELERDİR?

Güvenlik açıkları olduğunda veya bir saldırının hedefi olduğumuzda, çeşitli sonuçlar doğabilir:

- Ekipmanın başka amaçlar için kullanılması. Kurbanın cihazı, anonim olarak tarama bilgilerini toplamak, reklam göstermek veya diğer siber suçları işlemek için kullanılan bir botnet'e (bot veya "zombi" ağı) eklemek gibi şeyler yapmak için kullanılır. Enfeksiyon fark edilmeden kalmayı amaçlar ve genellikle kurban bunun farkında değildir.
- Fidye yazılımı tarafından cihazın ele geçirilmesi. Cihazın bir bölümüne erişimi engeller ve genellikle bir ödeme olmak üzere bir koşul talep eder.
- Hassas verilere veya kişisel bilgilere erişim. Kişisel bilgilerin (şifreler, fotoğraflar, banka bilgileri, kimlik belgeleri vb.) çalınmasının çeşitli amaçları olabilir ve genellikle saldırganın daha fazla müdahalesini gerektirir. En zararlı sonuçlardan bazıları, cinsel şantaj veya kimlik hırsızlığından, siber zorbalığa veya kamera veya mikrofonu etkinleştirerek casusluğa kadar uzanır.
- Aldatma ve dolandırıcılık. Aldatma sonrasında, mağdur para veya diğer dijital varlıkların çalınmasına maruz kalır ve hatta siber suçlara karışabilir.

UNUTMAYIN?

- Cep telefonları, tabletler ve bilgisayarlar, internete bağlandıklarında savunmasız hedefler haline gelen cihazlardır.
- İnternet üzerinden farklı kanallar aracılığıyla bize ulaşabilen ve çeşitli olumsuz etkileri olan birçok bilgisayar tehdidi (kötü amaçlı yazılım) türü vardır.
- Cihazlarınız enfekte olduğunda veya saldırıya uğradığında, farkında olmasanız bile, ciddi kişisel sonuçlarla karşılaşabilirsiniz.
- Kendi siber güvenliğinizi korumak, yeni koşullara ve uygulamalara uyum sağlamayı gerektiren günlük bir kişisel görevdir.
- Başkalarını da dikkate almanız ve desteklemeniz çok önemlidir. Onlar korunursa, siz de daha güvende olursunuz, çünkü hepimiz birbirimize bağlıyız.
- Güvende kalmak için, tüm cihazlarınızda (cep telefonları, tabletler veya bilgisayarlar) bir güvenlik veya antivirüs programına ve çevrimiçi hizmetlerinize, profillerinize ve uygulamalarınıza erişmek için güvenli şifrelere sahip olmanız çok önemlidir.

KÖTÜ AMAÇLI YAZILIM

Tanım

Genel bir tanım olarak, kötü amaçlı yazılım, bilgisayarlara ve bilgisayar sistemlerine birçok farklı yolla bulaşan ve rahatsız edici, zararlı, hatta yıkıcı veya onarılamaz etkilere sahip olabilen bilgisayar kodu veya yazılımıdır.

Başlangıçta bu zararlı yazılımın cihazda farklı derecelerde hasara neden olma (bilgileri silme, rahatsız edici bir uyarı penceresi gösterme, programlamada hatalar gösterme veya bulma vb.) gibi açık bir amacı olmasına rağmen, günümüzde varlığı kasıtlı olarak gizlidir ve çok sık olarak kar amacı güden suç faaliyetleriyle ilişkilidir. Enfekte olmuş kişiler ve cihazlarıyla tam, gizli ve görünür bir uyum içinde birlikte yaşayabilir.

Daha önce gruplandırılan ve genel olarak "bilgisayar virüsü" olarak bilinen bu terimden türetilen, günümüzde daha uygun başka tanımlar da vardır: kötü amaçlı yazılım, zararlı yazılım veya kötü amaçlı kod.

Genel Özellikler

Temelde bir bilgisayar "virüsü" biyoloji alanındaki karşılığıyla karşılaştırılabilir: diğer organizmaları enfekte eder, birçok farklı şekilde yayılır, bileşimi ve görünümü değişir, farklı belirtiler gösterir ve bunların hepsi hastalığa neden olmaz.

Kötü amaçlı yazılımlar cihazlarımıza birçok farklı şekilde girebilir. Bazıları, "sahte" bir bağlantıya tıklamak, kodun gömülü olduğu bir dosyayı veya uygulamayı indirmek, açmak veya yüklemek gibi kullanıcının müdahalesini veya bir tür eylemini gerektirir. Diğer kötü amaçlı yazılım türleri ise kullanıcının ihmali, dikkatsizliği veya yanlış bilgilendirmesi sonucu başkaları tarafından "enjekte edilir". Örneğin, cihazlardaki önceden ayarlanmış şifreleri değiştirmeyerek, kolayca kırılabilen bir şifre kullanarak vb. yöntemlerle gizlice giriş yaparlar.

Cihazlarımıza yüklediğimiz işletim sistemleri ve yazılımlar, bilgisayar kodu oldukları ölçüde, programlama hataları içerebilir ve ayrıca başkalarının içeri girmesine olanak tanıyabilir.

Yayılma yöntemleri çeşitlidir ve şunları içerir:

Diğerlerinin yanı sıra, USB sürücüler, ekli e-postalar vb.

Kötü amaçlı yazılımlar da programlama kodu olduğundan, çalıştığı her tür cihazı (masaüstü bilgisayarlar, dizüstü bilgisayarlar, tabletler, akıllı telefonlar, yönlendiriciler vb.) etkileyebilir; bu nedenle güvenlik önlemleri uygulanırken bunların hepsini dikkate almak tavsiye edilir.

Bu kötü amaçlı kodun oluşturulmasının ve dağıtımının arkasında insanlar olduğu ve bu nedenle amaçlarını belirlemenin zor olduğu unutulmamalıdır. Örneğin, bir truva atı gibi bazı kötü amaçlı yazılımlar, ciddi zarara yol açma niyeti olmaksızın bir grup öğrenci tarafından şaka veya deney olarak veya yasal olarak kurulmuş şirketlerin yazılımlarındaki veya cihazlarındaki güvenlik açıklarını kanıtlamanın bir yolu olarak programlanmış olabilir. Bununla birlikte, günümüzde bundan büyük bir iş yaratıldığı ve tek başına veya ekipler halinde organize olmuş kişilerin, mali kazanç elde etme amacıyla suç işlemekten çekinmediği şüphesizdir.

Günümüzde en tehlikeli ve gelişmiş tehditler hibrit yapıdadır. Özellikleri ve işlevselliği birleştirirler ve koruma yazılımı (genellikle antivirüs olarak bilinir) geliştiren şirketler tarafından analiz edilmelerini zorlaştırmak için cihazı silip yeniden başlattıktan sonra yeniden yükleme teknikleri kullanırlar.

Zararlı Yazılım Türleri

Çeşitli kötü amaçlı yazılım türleri vardır ve sınıflandırmaları genellikle yayılma biçimlerine dayanır, ancak alternatif olarak oluşturdukları tehlikeye göre de derecelendirilirler. Aşağıda en yaygın veya genel yayılma yöntemlerine sahip olanlar yer almaktadır.

Virüsler ve solucanlar (bulaşıcı kötü amaçlı yazılımlar)

- Bunlar diğer dosya ve programları enfekte ederek, enfekte cihazda kendilerinin kopyalarını oluşturmak üzere değiştirirler.
- Bunlar ayrıca dosya silme veya reklam gösterme gibi diğer eylemleri gerçekleştirmek üzere programlanabilirler.
- Virüslerin yayılması için kullanıcı müdahalesi gereklidir.
- Solucanlar kendilerini otomatik olarak çoğaltarak bir makineden diğerine yayılırlar.

Truva atları (gizli kötü amaçlı yazılımlar)

- "Zararsız" gibi görünerek, kullanıcıyı çalıştırmaya davet ederler ve diğer zararlı programlar için bir geçit oluştururlar.
- Kendilerini çoğaltamazlar ve kendi başlarına yayılamazlar, bu nedenle kullanıcı müdahalesi gereklidir.
- Eylemlerini fark edilmeden gerçekleştirirler.
- Kullanıcıların gizliliğini ve güvenliğini tehlikeye atarak veya çalışmalarını engelleyerek, uzaktan bilgi toplar veya ana bilgisayarını kontrol ederler.

Casus yazılım (veri toplayan kötü amaçlı yazılım)

- Kurulduğu cihazdan bilgi toplar ve bu bilgiyi onu yerleştiren kişiye iletir.
- Kullanıcının internetteki davranışlarını, verilerini, iletişim bilgilerini, kullanım alışkanlıklarını, ziyaret ettiği sayfaları, çalıştırdığı uygulamaları, bağlantı ayrıntılarını, cihazda kurulu uygulamaların listesini vb. izleyebilir.
- Banka hırsızlığından kimlik hırsızlığına kadar ciddi sonuçlar doğurabilir.

Diğer ilgili kötü amaçlı yazılım türleri şunlardır:

Sahtekar yazılım: Genellikle internetten fark edilmeden indirilir ve kurulur ve kullanıcıyı cihazının virüs bulaştığına inandırarak, ücretsiz bir deneme sürümü ve sözde enfeksiyonu kaldırmak için ücretli bir sürüm yüklemeyi teklif eder.

Fidye yazılımı (kriptovirüs, korsan yazılım): Bunlar, kullanıcının önemli dosyalarını şifreleyerek (şifreleyerek veya kodlayarak) erişilemez hale getiren ve ardından "engellenmiş" veya "şifrelenmiş" bilgilere tekrar erişim sağlamak için parola almak üzere büyük bir "fidye" ödemesi talep eden programlardır.

Genel Önlem Yönergeleri

Günümüzde gençleri tehdit eden bazı tehlikelerden kaçınmak için temel güvenlik önlemlerini teşvik ettiğimiz gibi, hepimizin sadece kendi değil, başkalarına ait de çok miktarda hassas bilgi ve veri taşıdığını göz önünde bulundurarak, öğrenciler

arasında cihazlarının korunmasını teşvik etmeliyiz.

Aşağıda çocuklar ve gençler için bazı genel öneriler bulunmaktadır:

- Her şeyden önce, özellikle arkadaşlardan, bilinmeyen kişilerden veya kuruluşlardan gelen beklenmedik mesajlar ve e-postalar söz konusu olduğunda, internette herhangi bir iletişim veya etkileşimle karşı karşıya kaldığınızda dikkatli, eleştirel düşünme ve sağduyu kullanın.
- Güvenilmez web sitelerinden yazılım indirmek risklidir, bu nedenle güvenilir bir üne sahip yasal olarak kurulmuş şirketlerin indirme hizmetlerini kullanmak daha tavsiye edilir. Şüphe durumunda, dosyaları açmamak veya çalıştırmamak ve güvenilirliğini veya doğruluğunu başka yollarla kontrol etmek her zaman en iyisidir. İndirilen, açılan veya çalıştırılan şeylerin ne olduğunu takip edin.
- Kendi cihazlarınızı tanımak, nasıl çalıştıklarını ve "normal" şekilde nasıl davrandıklarını anlamak, kötü amaçlı kodun varlığını tespit etmenize yardımcı olabilir. Olağandışı veya garip davranışlar bir enfeksiyona işaret edebilir ve yakın zamanda yeni bir program yüklediyseniz veya itibarsız web sitelerinde gezindiyseniz özel dikkat göstermeniz önerilir.
- Tüm cihazlarda, kullanılan işletim sisteminden bağımsız olarak, potansiyel saldırılara karşı gerçek zamanlı koruma sağlayan bir "antivirüs" yazılımının her zaman kurulu olması çok önemlidir. İnternet etkileşimlerimizden kaynaklanan tehditleri her zaman tespit etmenin yanı sıra, flash sürücülerde, harici sabit disklerde veya ekipmanımıza bağlı diğer donanım türlerinde de bunları tespit edebilir. Ayrıca, bilgisayarın düzenli olarak tam taramasını yapmayı ve antivirüslerin sınırlamaları olduğunu ve yanılmaz olmadığını, bu nedenle korunmamız için tamamen onlara güvenmememiz gerektiğini unutmamalıyız.
- Yazılımlarımızı (işletim sistemi, tarayıcılar, uygulamalar vb.) güncel tutmak da aynı derecede önemlidir, çünkü koddaki tespit edilen hatalar genellikle bu güncellemelerde düzeltilir ve diğer kişilerin bu hataları veya güvenlik açıklarını kullanarak cihazlarımıza erişmesini engeller.
- Cihazları ve işletim sistemlerini, programları, uygulamaları ve hizmetleri, kullanmaya başlamadan önce bile mümkün olan en "kapalı" veya kısıtlayıcı şekilde kurmak, herhangi bir izinsiz girişi önlemek için önerilen bir stratejidir. Bluetooth veya konum servisi gibi cihazları ve kullanıcılarını açığa çıkaran işlevler yalnızca gerektiğinde etkinleştirilmeli ve varsayılan olarak devre dışı bırakılmalıdır.

- Cihazlara, ağlara ve diğer hizmetlere giriş yapmak için basit ve kolayca kırılabilen veya tespit edilebilen şifreler kullanmak çok yaygındır. Zor veya güçlü şifreler kullanmak, evinizdeki kilit türü kadar önemlidir. Tanınabilir kalıplar kullanarak (8 veya daha fazla karakter uzunluğunda harf, rakam ve sembollerini birleştirmek önerilir) veya parola oluşturma hizmetlerini kullanarak, kırılma bile en azından başkalarının kırmasını zorlaştıracak bir anahtar oluşturmanıza yardımcı olacaktır. Hatırlatıcı kurallar veya tüm anahtarlarınızı içeren parola korumalı veya şifrelenmiş tek bir dosya kullanmak, bunları sorunsuz bir şekilde hatırlamanıza yardımcı olabilir. Her durumda, günümüzde neredeyse tüm hizmetler, unutulması durumunda çok basit bir parola kurtarma seçeneği sunmaktadır.
- Son olarak, dosyalarımızın (özellikle kaybolması ciddi zarara yol açacak olanların) düzenli yedeklerini almanın son derece önemli olduğunu nadiren düşünüyoruz. Bu nedenle, dosyalarımız veya cihazlarımız herhangi bir nedenle erişilemez hale gelirse, bunların kaybının sonuçları en aza indirilecektir.

Önleme kadar önemli olan bir diğer şey de, önleyici önlemlerimizi alt etmeyi başaran bir tehdidin erken tespiti ve ardından gelen iyileştirici eylemlerdir.

Tespit ve Eylemler

Önleyici tedbirlerin yanı sıra, çocuklar potansiyel siber güvenlik sorunlarını tanımlayabilmenin ve en azından temel düzeyde bu gibi durumlarda ne yapılması gerektiğini bilmenin öneminin farkında olmalıdırlar.

Kötü amaçlı yazılım sistemimize girdikten sonra, onu tespit etmek her zaman kolay değildir. Ancak, cihazlarımızda şu belirtilerden bazılarını tespit edersek sorun yaşıyor olabiliriz:

- Çok fazla ısınıyor.
- Çok fazla pil tüketiyor.
- İnternette gezinirken görünürde hiçbir sebep yokken açılır pencereler beliriyor.
- Tarayıcımız bizi istenmeyen web sitelerine yönlendiriyor.
- Dosyalar ve programlar, görünürde hiçbir sebep yokken ve biz olağanüstü bir şey yapmadan kayboluyor veya devre dışı kalıyor.

Enfeksiyonun ciddiyetine ve yeterli bilgiye sahip olup olmadığımıza bağlı olarak, bazı önlemler alınabilir:

- Antivirüs/kötü amaçlı yazılım önleme yazılımı kullanarak derinlemesine tarama ve temizleme işlemi gerçekleştirin. Cihazınızda antivirüs yazılımı yüklü değilse, cihazlarınızın hızlı bir çevrimiçi taramasını yapmak için ücretsiz araçlar sunan veya

daha kapsamlı bir arama yapmak için yüklenebilecek deneme sürümleri sunan birçok şirket bulunmaktadır. İlk aşamada hiçbir şey bulunmazsa, farklı tespit araçları kullandıkları için farklı bir antivirüs kullanarak daha fazla tarama yapmanız önerilebilir.

- Kullanılan internet tarayıcısını temizleyin (çerezler, yüklenmiş olabilecek eklentiler...)
- Özellikle yükledikten sonra cihazda sorunlar tespit etmeye başladıysanız, programları, eklentileri veya uygulamaları kaldırın.
- Uzman profesyonellerden yardım alın.

GÜVENİLİR OLMAYAN BAĞLANTILAR

Cep telefonları ve tabletler aracılığıyla hareket halindeyken internet kullanımı giderek yaygınlaşıyor. Bu, özellikle küçük çocukların, bağlanmak için genellikle Wi-Fi olmak üzere bir ağ aradıkları anlamına geliyor. Okul çocukları, bu bağlantı noktalarının da bir tehdit oluşturabileceği konusunda uyarılmalıdır.

Kablo, Wi-Fi vb. aracılığıyla herhangi bir yerden internete bağlanırken,

Milyonlarca birbirine bağlı cihazdan oluşan bir ağa erişiyor ve katılıyorsunuz. Bu cihazlar, genellikle, yalnızca "açık" içeriğe erişmek ve göz atmak için kendi cihazınızdaki gibi güvenlik önlemleri uygulamıştır. Ancak, bu güvenlik önlemleri yanlış ayarlanmış olabilir veya hiç ayarlanmamış olabilir ya da kırılmaya çalışılacak kadar cazip olabilir ve diğer kişiler, iletişimlerimizi ele geçirmenin yanı sıra, bu bağlantı yoluyla cihazlarımıza erişebilir ve bu da tehlikeler doğurabilir. Aynı şekilde, internet bağlantısı olmasa bile, cihaz ağları benzer özelliklere ve risklere sahiptir.

Evimizde ve okulumuzda kendi cihazlarımızın ve bağlantılarımızın yapılandırmasını kontrol edebilirsek bile, genellikle internet bağlantısı olsun veya olmasın, kullanıcıların ağlarına erişmesine izin verilen kamu veya özel yerlerde hangi güvenlik önlemlerinin alındığını bilmiyoruz.

Özellikle gençler arasında, internet sağlayıcılarının belirli sınırlar dahilinde sağladığı veri kullanımından tasarruf etmek için, "Wi-Fi'yi çaldıkları" inancıyla açık veya kolayca kırılabilen Wi-Fi bağlantıları bulmak amacıyla yazılım yüklemek yaygın bir uygulamadır. Bunu yaparak, risklerin farkında olmazlar ve cihazlar arasında iletişim kurmak ve sonuç olarak bağlı olanlara erişim sağlamak için bağlantılarını "açan" diğer kişilerin kurduğu tuzağa düşme riskiyle karşı karşıya kalırlar.

Benzer şekilde, ücretsiz veya açık bağlantılar dolandırıcılık niyetlerini gizleyebilir. Kaçınılması gereken en önemli davranış, açık bir halka açık Wi-Fi ağına (şifresiz)

bağlanmaktadır, çünkü bu, ücretsiz ağındaki bir siber suçlu tarafından sunulduğu ve sizi aradığınız ağı olduğunu düşündüren yanlış bir isim altında sunulduğu bir tuzak olabilir.

SAHTEBAĞLANTILAR

Sıklıkla birçok sonuç veren yaygın bir tehdit, masum ve bazen de incelikten yoksun bir görünüm altında sahte bağlantılar sağlamak ve kullanıcıları hassas verilerini vermeye zorlayarak gerçek aldatıcı durumlara yönlendirmektir. Çocuklar genellikle kendi nakit paraları olmadığı için mali nedenlerle siber suçun hedefi olmasalar da, bu tekniklere aşına olmaları önemlidir, çünkü bunlar çevrimiçi alışveriş veya video oyunları gibi faaliyetleriyle ilgili ödeme sistemlerinde uygulanabilmektedir.

Nasıl Çalışırlar?

Doğrudan (e-posta, WhatsApp, forumlar veya ağlar aracılığıyla) veya dolaylı olarak (bannerlar, reklamlar, gizli kötü amaçlı yazılım indirme vb.) alınırlar ve etkinleştirildiklerinde genellikle kullanıcının bir form doldurmasının istendiği gerçek web sayfalarıyla aynı olan web sayfalarına yönlendirirler. Kullanıcı formu doldurup istenen verileri verdiğinde, bu veriler siber suçlular tarafından ele geçirilir.

Bu mesajların bazıları empati veya dayanışma duygularımıza (uzak bir ülkede yaşadıkları için miraslarını nakde çevirmekte zorlanmaları), merakımıza (“sizi arkadaş grubundan kimin çıkardığını öğrenin”), saflığımıza (“araba kazandınız”) hitap eder ve uyarı veya tehditler (“sistem güncellemelerini yüklemek için gerekli verilerin onaylanması”) içerir. Otomatik olarak gönderilen milyonlarca mesaj arasında, birçoğu birçok insanı kandırmayı başarır.

Siber suçlular için en karlı dolandırıcılık tekniklerinden biri, aşağıda özetlendiği gibi çalışan kimlik avı (phishing) olarak adlandırılır:

- Hesap numaraları, şifreler ve diğer hassas verileri elde etmek için bir bankanın görüntüsü farklı bir görüntüyle değiştirilir.
- Bankanın logosunu gösterebilirler, ancak genellikle kişiselleştirilmemişlerdir, çünkü toplu olarak gönderilirler ve genellikle dil bilgisi ve yazım hataları içerirler.
- Bağlantılar, kullanıcıları e-postalardan “https” ile başlamayan sayfalara yönlendirir ve kilit simgesi görüntülenmez (bu, dijital sertifikaya sahip olmadıkları anlamına gelir).
- Yönlendirildikleri sayfa, bankanın orijinal sayfasına çok benzer.

Önleme Tedbirleri

Sahte bir bağlantıya girme olasılığını azaltmak için şunlar önerilir:

- E-postalarda, mesajlarda veya web sitelerinde verilen bağlantılara tıklamak yerine, URL'yi veya web sayfası adresini tarayıcıya yazın.
- Sayfanın "https" protokolünü (sonunda bir "s") kullandığından ve dijital sertifikayla ilgili kilit simgesini gösterdiğinden emin olun. Bu simge veya ikon genellikle web tarayıcınızın durum çubuğunun altında veya adres çubuğunun üstünde görünür. Üzerine tıklamak, özetle, erişilen web sitesinin sahibi hakkında bilgi sağlayan, belirli bir yetkili tarafından imzalanmış bir sertifika olan dijital sertifikanın açıklamasını içeren bir pencere görüntüler.
- Bankaların veya işletmelerin asla e-posta yoluyla kişisel bilgiler istemeyeceğini unutmayın.
- Gizli bilgileri girmekten kaçının ve şüpheniz varsa doğrudan şirketle iletişime geçin.
- Sağduyuyu kullanın; kimse bir şeyi karşılıksız vermez.

CİHAZLARA YETKİSİZ ERİŞİM

Cep telefonu taşınabilir bir cihazdır.

Sürekli kullandığımız ve bu nedenle unutulabilen, kaybolabilen hatta çalınabilen bir cihazdır. Gözden uzak bir yerde saklanırsa, bir süre sonra istenmeyen kişilerin eline de geçebilir. Öğrencilerin bunu düşünmelerini ve gizlilik açısından da akılda tutmalarını teşvik etmek önemlidir. Bu durumda, aşağıdaki gibi çeşitli önleyici tedbirler göz önünde bulundurulmalıdır:

- Cihaza yalnızca meşru sahibinin erişebilmesi için parola, desen veya PIN ve/veya dijital erişim ayarlayın.
- Uygulamaların, tarayıcıların ve programların parolaları cihazın hafızasına kaydetmesini engelleyin, böylece cep telefonunu ele geçiren diğer kişiler otomatik olarak erişim sağlayamaz veya kendilerine ait olmayan bir kimlikle işlem yapamazlar.
- Cihazları, cep telefonlarını ve dizüstü bilgisayarları bulmak ve izlemek için kullanılan uygulamalar, programlar ve hizmetler vardır ve çalınmadan veya kaybolmadan önce yüklenirse, bulunmalarına yardımcı olur.

GÜVENLİ ŞİFRELER

Şifreler, yasa dışı veri erişimine (konuşmalar, resimler, kişiler vb.) ve bize zarar vermek için kullanılabilecek kişisel hizmetlere karşı ilk koruma hattıdır. Şifreler siber güvenlikte ilk bariyer, dijital yaşamımızın kapısıdır ve bu nedenle güçlü olmalıdırlar. Şifre seçimi, sık sık alınması gereken önemli bir karardır. Şifreler, yasa dışı veri

Şifreler, kişisel bilgilere erişim kapısı açtıkları için gizlilikle eşdeğerdir. Ancak, belirli verilere erişim, kimlik hırsızlığı veya şantaj gibi çeşitli şekillerde ciddi zararlara yol açabileceğinden, şifreler sahibinin güvenliğiyle de ilgilidir. Sonuç olarak, şifreler dijital hayata açılan kapıdır ve bu nedenle güçlü olmalıdırlar. Erkekler, kızlar ve ergenler bu bariyerleri nasıl güçlü bir şekilde oluşturacaklarını bilmelidirler.

Sekiz Adımda Güvenli Bir Şifre

1. En az 8 karakter içermelidir.
2. Tahmin edilmesi kolay olmamalıdır (isim, doğum tarihi vb.).
3. Büyük ve küçük harfler içermelidir.
4. Sayı ve harf içermelidir.
5. Herhangi bir cihaza kaydedilmemelidir. Her istendiğinde manuel olarak girilmelidir.
6. Bu, aile dışında kimseyle paylaşılması gereken bir sır olmalıdır.
7. Düzenli olarak değiştirilmelidir.
8. Her hizmet, sosyal ağ veya uygulama için farklı olmalıdır.

SİBER GÜVENLİĞİNİZE YÖNELİK TEHDİTLERE KARŞI KENDİNİZİ KORUMAK İÇİN ÖNERİLER

Şimdiye kadar görüldüğü gibi, siber güvenliğin çeşitli yönleri herkesin (çocuklar, ergenler ve yetişkinler) dikkate alması gereken hususlardır. Bunlar, öğrencilere kolayca aktarılacak sekiz öneride özetlenebilir:

- İnternete bağlanmak için kullandığınız tüm cihazlarda (bilgisayar, cep telefonu veya tablet) antivirüs yazılımı kullanın. Birçok ücretsiz ve tüm işletim sistemleriyle uyumlu antivirüs yazılımı mevcuttur.
- İşletim sisteminizi ve uygulamalarınızı güncel tutun.
- Uygulama indirirken, yetkili mağazalardan indirin. Şüpheli yasal veya kaynaklardan gelen yazılımlara güvenmeyin, çünkü kötü amaçlı yazılım içerebilirler.
- Bilinmeyen kişilerden veya kaynaklardan gelen bağlantıları veya beklenmedik dosyaları açmaktan kaçının. Bunları otomatik olarak indirmeyin.
- Şifrelerinizi nereye girdiğinize ve kimin istediğine özellikle dikkat edin.
- Bir web sayfasının adresi “https” ile başlıyorsa, güvenli ve güvenilir olduğu anlamına gelir.
- Herkese açık Wi-Fi ağlarına bağlanmak risklidir. Kritik hiçbir şey yapmamaya çalışın, çünkü iletişimleriniz gözetlenebilir.
- Bluetooth gibi hizmetlerin, yalnızca kullanacağınız zaman cep telefonunuzdan

bilgi paylaşmasına izin verin.

- Dikkatli olun ve etkileşimde bulunduğunuz kişilerin ve kullandığınız hizmetlerin bilgilerini çapraz kontrol edin. Bilgileri veya referansları çevrimiçi olarak arayarak çapraz kontrol etmek, dolandırıcılık ve sahtekarlıkları ortaya çıkarmaya yardımcı olabilir.

SİBER ZORBALIK



Siber Zorbalık

Genellikle siber zorbalık olarak bilinen akranlar arasında çevrimiçi taciz şüphesiz ciddi bir sorundur. Ergenler ve hatta küçük çocuklar arasında giderek artan ve okul bağlamının ötesinde sonuçları olan çok özel bir dijital şiddet biçimidir.

Zorbalığa uğrayan kişinin çektiği acı son derece yoğundur. Üzüntü, izolasyon, özgüven ve benlik saygısı eksikliği, uyku ve yeme bozuklukları, psikosomatik bozuklukların başlangıcı vb. şeklinde kendini gösterebilir. Bu durum, mağdur olanlarda derin ve kalıcı bir yara izi bırakır.

UNUTMAYIN

- Siber zorbalık, çocukların internette karşılaştığı en önemli zorluktur. Ciddi zararlara neden olur, oldukça düzenli olarak meydana gelir ve önlenmesi ve durdurulması son derece zordur.
- Fiziksel saldırganlığın olmaması, mağduriyetin veya zararın verilmemesi anlamına gelmediğinin farkında olmak önemlidir.
- İnternet çok güçlü bir araç olduğundan, zarar vermek için kullanıldığında etkileri yıkıcı olabilir. Mağdurlar ve saldırganlar arasında önemli bir güç dengesizliği vardır.
- Bu tür akranlar arası dijital şiddet üç yönü kullanır: yapması kolaydır, anında sonuçları vardır ve her zaman ulaşılabilir durumdadır.
- Siber zorbalığa maruz kalan kişiler kendilerini izole etme eğilimindedir, bazen durumlarından dolayı suçluluk duyarlar. Genellikle erken aşamalarda yardım istemezler.

SİBER ZORBALIĞIN TANIMI VE AÇIKLAMASI

Siber zorbalık, internet üzerinden (sosyalağlar, video oyunları, anlık mesajlaşma, web sayfaları...) bir veya birden fazla kişi tarafından, benzer yaşta ve okul ortamında kendileriyle ilişkili bir mağdura karşı kasıtlı, tekrarlayan ve sürekli bir şekilde gerçekleştirilen tacizdir. Bu kişiler, mağdur üzerinde üstünlük kurmuş veya üstünlük sağlamış olabilirler. Bu üstünlük, cezasızlık yoluyla veya kontrol dayatarak gerçekleşebilir. Genellikle okul zorbalığı ve siber zorbalık el ele gider, ancak her zaman değil.

Bu, çeşitli şekillerde olabilir: yanlış bir söylenti yayınlamak, alaycı veya aşağılayıcı bir resim paylaşmak, bir mesajlaşma grubundan çıkarılmak, bir sosyal ağda şifre çalmak ve başkalarını taklit ederek hakaret etmek gibi. Saldırıların tekrarı her zaman aynı kişi tarafından gerçekleştirilmez; basit bir "Beğen" veya incitici bilgi paylaşımıyla katılan birkaç farklı kişi olabilir.

İşaretler Nelerdir?

Gerçek şu ki, interneti kullanarak erkek, kız ve ergenleri incitmenin yolları hayal gücü kadar çeşitli olabilir. İnternetin hem bir sosyalleşme ortamı hem de diğer bağlamlara çapraz bir unsur olması, daha geniş bir çeşitliliğe olanak tanır. Siber zorbalığın en yaygın belirtileri şunlardır:

- Kışkırtma: Herhangi bir yapıcı amaç olmaksızın bir foruma saldırgan mesajlar göndermek.
- Meta/Facebook gibi çevrimiçi hizmet yöneticilerine kasıtlı olarak bildirimde bulunmak. Sosyal ağların, kayıt işlemi sırasında kabul edilmesi gereken bir kullanım şartları politikası vardır. Bu politika, hakaret veya özel görüntülerin yayınlanması gibi belirli davranışları yasaklamaktadır. Aynı zamanda, bu ihlalleri bildirmek için kullanıcı topluluğundan belirli bir kanal veya form kullanarak yardım istemektedirler. Kullanıcılar, kullanım şartlarını ve koşullarını ihlal eden bir durumu sahte bir şekilde simüle ederek veya oluşturarak başkalarını bildirebilir ve hatta bildirilen profilin yasaklanmasını veya kapatılmasını sağlayabilirler.
- Kullanıcıların anonimliğini teşvik eden gruplara gönderilebilecek saldırgan ve hakaret içeren mesajlar yoluyla takip ve taciz. Örneğin, WhatsApp grupları gibi uygulamalar (gerçek isim kullanarak veya anonim olarak başka bir kişiye yönelik düşünceler veya duygular hakkında yorumların paylaşılabilirdiği bir internet sitesi).
- Birinin kimliğine bürünmek veya kimliğini kullanarak başkalarının önünde saldırgan veya tehlikeli bir şekilde hareket etmesini engellemek için şifre çalmak.
- Sadece rahatsızlık vermek amacıyla birini cinsel olarak taciz etmek, örneğin pornografik görüntüler göndermek.
- Tehdit yoluyla gözdağı vermek. Bunlar kelimelerden veya fiziksel bir saldırganlığın gösterildiği bir videoya basit bir bağlantıdan oluşabilir.
- Başka bir kişiyi veya grubu sahte bir şeyin gerçek olduğuna inandırabilecek, itibarı ve arkadaşlıkları zedeleyebilecek şekilde aşağılamak, alaycı sayfalar oluşturmak veya yanlış bilgi veya haber yaymak.
- Birini kasıtlı olarak çevrimiçi etkinliklerden dışlamak, örneğin onu sınıf içi anlık mesajlaşma grubuna (örneğin WhatsApp) dahil etmemek.

Bu sorunun okul ortamındaki erkek, kız ve ergenlerde nasıl tespit edilebileceğini bilmek bizim için önemlidir:

- Örneğin, yetersiz gerekçelerle okula gitmemek.
- Dikkat süresinin azalması.
- Ani ruh hali değişimleri.

- Üzüntü, ilgisizlik veya kayıtsızlık anları.
- Anlık saldırganlık patlamaları.
- Arkadaş veya sosyal ilişkilerin olmaması.
- Sınıfta minimum iletişim veya izolasyon.

Zorbalık Ve Siber Zorbalık Arasındaki Farklar

Siber zorbalığın ilk belirtilerini ve risk faktörlerini etkili bir şekilde belirleyebilmek için, öğretmenlerin akranlar arasında siber mağduriyetin çeşitli türleri arasındaki farkı bilmeleri önemlidir.

Mağdurun acı çekmesi ortak sonuç olsa da, siber zorbalıkta geleneksel zorbalığa kıyasla çok önemli ayırt edici özellikler vardır.

Mağdur her zaman, her yerde saldırganlığın menzilindedir. Bağlı olmasa bile, sosyal ağlardaki profili hakaret içerikli mesajlar alabilir. Bu durum, forumlarda, mesajlaşma gruplarında veya sosyal ağ resimlerinde olumsuz yorumlar nedeniyle kimliklerinin veya dijital itibarlarının zarar görmesiyle aynı anda bile gerçekleşebilir.

- Zorbalık liderliği daha yaygın ve daha fazla insan buna katılma eğilimindedir. İnternet, başka bir okuldan olsalar bile herkesin saldırganlığa katılmasına olanak tanır ve internetteki hemen her şey gibi, işbirliği içinde veya paylaşımlı bir şekilde yapılabilir.
 - Saldırganlıklar daha fazla insan tarafından algılanır ve daha uzun sürer. Ancak, aileler ve eğitim camiası için daha az görünürdürler. Örneğin, incitici, kötü veya tehdit edici resimler yayınlayan zorbalığa uğrayan öğrenci gibi davranan sahte bir Facebook profili oluşturmak ve paylaşmak az çaba gerektirir ve büyük bir etkiye sahiptir.
 - Verilen zararın algılanması daha düşüktür, çünkü tacize uğrayan kişinin acısı genellikle doğrudan görünmez. Ekranlar, mesafe ve hatta zaman söz konusu olduğunda empati geliştirmek kolay değildir. Şaka olarak yazılan bir tehdit, belirli bir zamanda ve belirli bir bağlamda alıcıya en ağır ceza gibi görünebilir.
 - Saldırganların ve kurbanların profilleri çok çeşitlidir. Net bir kalıp yoktur.
 - Herkesin zarar verme kapasitesi vardır. Hem siber zorbalığa maruz kalan hem de siber zorbalık yapan veya hatta buna öncülük eden insanlara rastlamak yaygındır.
- Bu farklı karakterler, internetin öğrencilere sosyalleşme için hem bir kanal hem de bir bağlam olarak sunduğu farklılaştırıcı faktörlerden kaynaklanmaktadır.

Akranlar Arası Siber Zorbalığı Teşvik Eden Unsurlar

İnternet ve dijital yaşam, öğrenciler arasında şiddetin kolayca uygulanmasını sağlayan belirli özelliklere sahiptir. Siber zorbalığı durdurmaktan çok daha kolaydır. Siber zorbalık çok farklı biçimler alır ve diğer yasa dışı davranış türlerine göre cezasız kalma olasılığı daha yüksektir. Siber zorbalık yapmayı "çekici" kılan şu katalitik faktörler belirlenebilir:

- İnternetin sağladığı anonimlik (kendini tanıtmama), taklit (başka biri gibi davranma) ve sahtekarlık (kurgusal bir kimlik benimseme), bir dizi olasılık sunar ve daha büyük bir cezasızlık hissi verir.
- Çevrimiçi içeriğe erişimin ve üretimin anlık olması, kalitesi, gücü ve fiyatı, cihazların bulunabilirliği ve düşük maliyetiyle birlikte, potansiyel bir tacizcinin ulaşabileceği değerli bir silah stoğu oluşturmaktadır. Bir bilgisayardan veya cep telefonundan her yerden dolaşmaya başlayabilir.
- Teknolojik becerinin akran grubunda olumlu bir şekilde değerlendirilmesi, bazılarının akran öğrencilerine zorbalık yaparak becerilerini sergilemek suretiyle kendilerine dikkat çekmelerine yol açabilir.
- Takip için yeni olanaklar yaratan ve ek önleyici çabalar gerektiren uygulamaların ve hizmetlerin sürekli ortaya çıkması. Yeni sosyal uygulamaların ortaya çıkmasıyla yeni zorbalık biçimleri ortaya çıkabilir.
- Siber zorbalığın sürekli değişen ve çeşitli biçimler alması, soruşturmayı ve ceza kovuşturmayı çok zorlaştırdığı için kanıtlanması zordur. Böylesine değişken bir ortamda, zorbaları tespit etmek ve eylemlerinin kanıtlarını elde etmek için uzun süreli standart protokoller oluşturmak zordur.
- Çevrimiçi video oyunlarının, gizliliği ve iyi bir birlikte yaşama ortamını korumayı hiç önemsemeden sanal topluluklar oluşturmak için yaptığı yatırım. Bunlar, bazı durumlarda iç sorumluluk yapıları ve düzenlemelerden yoksun görünen eğlence ortamlarıdır.
- Mağdurla gerekli kişisel temasın olmaması (bazen tanıdık bile değillerdir) veya zihinsel veya fiziksel olarak daha güçlü olmamaları. Bu, zorbalığa uğrayan ve zorba profillerinin olası kombinasyonlarının zamanla giderek artması anlamına gelir.
- Zorbaların kolayca "gruplandırılması". İnternette, gerçek veya hayali bir dava için savaşılmaya hazır insanları bulmak zor değildir; Bu, kendi başlarına veya başkasının başına gelebilir veya sadece bir zorba grubunun parçası olmak anlamına gelebilir.
- Farklı eylemlerin sonuçlarının farkında olmamak. Bir şaka olarak veya sinirlenme sonucu başlamış olabilir, ancak mağdurun alay konusu olduğu fotoğraf

beklenenden daha fazla yayılabilir. Ayrıca, mağdurun ruh halindeki hassas bir anla (diğer kişisel sorunlar, düşük özgüven vb.) çakışabilir. Bu nedenle, birisi amaçlanandan veya hayal edilenden daha fazla zarar verebilir.

- “Herkes yapar”, “Bunu kastetmedim” veya “Sadece ben değildim” gibi bahaneler. Bunlar, sorumluluktan kaçınmanın basit yollarıdır.
- Eylemlerinden sorumlu oldukları bir rol üstlenmek. Birisi bir kişiliğe büründüğünde ve internette kendini farklı biri olarak gösterdiğinde, ekranın her iki tarafında da sorumluluklarını ve vicdanlarını farklı şekilde görebilirler.
- Çevrimiçi yaşamın artan önemi. Bu, siber zorbalık eylemlerinin büyük bir etki potansiyeline sahip olduğu ve bundan kaçınmak için çok az fırsat veya yol olduğu anlamına gelir. Geçmişte internete bağlı olmak tesadüfi bir şeyken, gelecekte internetten kopuk olmak giderek daha çok anekdot niteliğinde olacaktır. Çevrimiçi olmak, zorbalığa maruz kalma ve zorbalık yaşama olasılığını artırır.

Kısacası ve ne yazık ki, siber zorbalık kolay, ucuz, her zaman el altında ve çok sık cezasız kalıyor.

YAŞAM BECERİLERİNİN ÖNEMİ

Yaşam becerilerine dayalı eğitim, günlük yaşamın talepleri ve zorluklarıyla başa çıkmak için yararlı olan beceriler konusunda eğitim vermeye odaklanır. Yaşam becerilerine dayalı eğitim, insanların daha sağlıklı ve mutlu bir yaşam sürme, sağlık ve refahı belirleyen faktörler üzerinde etkili olma ve aktif olarak katılım sağlama yeteneklerini geliştirmeyi amaçlamaktadır.

Daha adil, daha destekleyici ve eşitlikçi toplumlar inşa etmede rol oynarlar.

Yaşam için on temel beceri belirlenebilir:

- Öz farkındalık.
- Empati.
- Girişken iletişim.
- Kişilerarası ilişkiler.
- Karar verme.
- Problem ve çatışma yönetimi.
- Yaratıcı düşünme.
- Eleştirel düşünme.
- Duyguları ve hisleri yönetme.
- Gerilim ve stresi yönetme.

Duruma bağılı olarak farklı derecelerde müdahale etseler de, hepsi gereklidir. Öte yandan, dijital yaşam söz konusu olduğunda çeşitli düzeylerde önem taşırlar. Bu bağlamda, özellikle siber zorbalık ortamlarında, bunlardan bazılarının sınıfta geliştirilmesini teşvik edebiliriz. Birçoğu, belirli zararlı davranışlara karşı bir panzehir görevi görebilir.

Siber Bir Birlikte Yaşam İçin Bazı Temel Beceriler

Siber zorbalık, mağdur, saldırgan ve tanık olmak üzere tüm ilgili taraflar için büyük zorluklar yaratır. Siber zorbalık denklemindeki role bağılı olarak, yaşam becerileri hem önlemeye hem de başa çıkmaya yardımcı olabilecek öne çıkan yaşam becerileri şunlar olabilir:

- **Empati:** Kişilerarası ilişkiler söz konusu olduğunda bu çok önemlidir. Acı çektiklerini hissetmezsek empati kuramayız. Ekranlar ve mesafe, zararı algılamayı zorlaştırır.
- **Özgüven:** Düşük özgüven, aksi gibi görünse bile, zorbalığın tipik özelliğidir. Yüksek özgüven genellikle zorbalığa maruz kalanlar tarafından geliştirilmesi gereken bir beceridir.
- **Eleştirel düşünme:** Diğer beceri ve değerlere ek olarak, siber zorbalıktan kurtulmanın ilk adımı, onu "normal" olarak kabul etmeyi bırakmaktır. Normalleştirmeyi reddetmek, seyircileri harekete geçirmek için çok önemlidir.
- **Kendine güven:** Tanıklar, kendilerini rahat hissetmedikleri şeylere katılmaktan vazgeçebilecekleri bir konumda olmalıdırlar.

BİRLİKTE SİBER YAŞAM: BİLİNÇLİ, KALICI VE KOLEKTİF BİR MEYDAN OKUMA

İnternetin özellikleri, hem sınıf içinde hem de dışında saldırganlıkları daha kolay ve elverişli hale getiriyor. Bu nedenle, internetteki tüm insanlar arasında günlük olarak iyi bir birlikte yaşama ortamı oluşturulmalıdır. Bunu birlikte fark etmeliyiz. Bunu yapmak için sorumlu dijital vatandaşlık kavramını anlamak çok önemlidir. Bu, internette her zaman diğer insanları dikkate almak anlamına gelir ve hatta zorbalığa yol açabilecek herhangi bir çatışmayı proaktif olarak önlemeye çalışmak demektir.

Aşağıda, öğretmenlerin öğrenciler arasında birlikte siber yaşama ortamını ve sonuç olarak dijital refahlarını iyileştirmeleri için on ipucu bulunmaktadır.

Birlikte Pozitif Dijital Yaşam İçin On Kural

1. İnternetin tadını etik ve kibar bir şekilde çıkarın, internet görgü kurallarını kullanın. Kendinize de internet görgü kurallarını uygulayın. İnternet görgü kuralları, internette iyi ilişkiler kurmamıza yardımcı olan bir dizi öneridir. Bunlara uymak dijital birlikte yaşamı iyileştirir.

2. Başkalarını kamuya açık yerlerde rahatsız edebilecek ifadeler kullanmaktan kaçının.

İnternette söylenenler çok sık beklenmedik bir şekilde yayılır ve birileri için üzücü veya rahatsız edici olabilir.

3. Kendinizi kötü amaçlı yazılımlardan koruyun. Akıllı telefonunuzu kilitleyin ve şifrelerinizi koruyun.

Kendi bilgilerinize veya başkalarının bilgilerine istenmeyen erişimi önlemek önemlidir. Cihazları ve şifreleri korumak kimlik hırsızlığını önler.

4. Ekranın bu tarafında olmanın sizi korumadığının farkında olun.

Sadece bağlantıyı keserek durumların üstesinden gelebileceğinizi düşünmek akıllıca değildir. İnternetin çok geniş bir erişim alanı vardır.

5. Koruma seviyenizi artırmak için kişisel verilerinizi ve gizliliğinizi koruyun.

Bir kişi hakkında ne kadar çok bilgiye sahipseniz, zarar görme olasılığı o kadar yüksektir.

6. İnternette yüz yüze yapmayacağınız şeyleri yapmayın.

Bazen, ekranın diğer tarafındaki kişi, düşündüğünüzden daha yakın biri olabilir. Dil, yaş, ilgi alanları ve kültür hepsi yardımcı olur.

7. Saldırgan veya garip insanlardan uzak durun ve yeni kişilere dikkatli olun.

İnternette bazı insanlar sadece kıskırtmak ve zarar vermek ister. Özellikle sosyal ağlarınızda onlardan kaçınmak önemlidir.

8. Varsayımlardan kaçının. Yanılıyor olabilirsiniz.

Saldırgan bir eylem bazen kasıtlı değildir, yanlış yorumlanmıştır veya başka birine yöneliktir. Ayrıca kasıtlı bir aldatmayı da gizleyebilir.

9. Kıskırtmayı görmezden gelin. Ona kadar sayın ve cevap vermeden önce başka bir şey düşünün.

Saldırgan bir davranışa cevap vermek çatışmadan kaçınmaya yardımcı olmaz ve siber zorbalığa yol açabilir. Kötü niyetli ve internet erişimi olan biri ciddi zarara neden olabilir.

10. Çevrimiçi olarak taciz edildiğinizde, site veya hizmet yöneticisinden yardım isteyin.

Sosyal ağ siteleri ve oyunlar gibi birçok çevrimiçi hizmetin, kullanıcılarının saldırgan davranışlarını yasaklayan kullanım politikaları vardır.

ÖNLEYİCİ ÇALIŞMALAR

Siber zorbalık temelde bir değerler meselesidir. Ancak, bu değerler koşullu olabilir veya her durumda, bu değerlerin yokluğunun ne kadar yoğun bir şekilde tezahür edebileceği de önemlidir. Yaşam becerilerinin geliştirilmesine ek olarak, siber zorbalığı azaltmaya yardımcı olabilecek çeşitli eylem yolları vardır.

Gizliliği ve Siber Güvenliği Teşvik Etmek

Gizlilik ve siber güvenlik el ele gider ve bunlarla birlikte bireylerin güvenliği de gelir. İyi güvenlik ve gizlilik uygulamalarına sahip bir erkek, kız veya ergenin siber zorbalığa maruz kalma olasılığı daha düşük olacak veya bu siber zorbalığın daha az yoğun veya daha az sonuç doğurması daha olasıdır.

Yasal Sınırların ve Sorumlulukların Yayılması

Yasaların dışında kalanlar ve bu tür eylemlere girişenler için sonuçları hakkında farkındalık yaratmak çok önemlidir. Tehditler, hakaretler, sırların ifşa edilmesi ve kimlik hırsızlığı, siber zorbalık kapsamına giren ve kanunen cezalandırılabilen eylemlerdir. Bu durumun farkında olan bir ergen, siber zorbalığa karışmamaya veya zaten karışmışsa, bu davranışından vazgeçmeye veya yumuşatmaya karar verebilir. Öte yandan, mağdur yasanın kendi tarafında olduğunun farkındaysa, saldırgan eylemin kanıtlarını saklayabilir ve gerekirse yasal işlem başlatabilir.

Dijital Vatandaşlık ve İnternet Görgü Kurallarının Teşviki

Çocuklara ve ergenlere internetin sadece kullandığımız bir şey değil, yaşadığımız ve birlikte var olduğumuz bir yer olduğunu anlatmalıyız. Bu nedenle, bu yeni bağlamda proaktif bir rol oynamalı, dijital vatandaşlar olarak hareket etmeli ve bu harika sosyalleşme ortamından yararlanmamızı sağlayan hak ve görevlerimizi aktif olarak kullanmalıyız. İnternet, onu nasıl kullandığımıza bağlıdır.

Ortak sorumluluğu teşvik etmeliyiz. Bu doğrultuda, belirli bir dijital bağlamda keyif alma ve birlikte yaşama koşullarını iyileştirmek için belirli bir grup tarafından oluşturulan kurallar bütünü olan internet görgü kuralları kavramını da dahil edebiliriz. Benzer şekilde, daha büyük öğrencilerin daha küçük öğrencilere çevrimiçi ortamda sağlıklı kullanım ve olumlu bir arada yaşama konusunda rehberlik etme sorumluluğunu üstlendiği dinamikler oluşturmak, okul atmosferinde olağanüstü bir etkiye sahiptir.

Farklı Hedef Kitlelerine Yönelik Harekete Geçme Çağrısı

Genel olarak zorbalık veya siber zorbalık mağdurları veya tanıkları olarak tanımlanan farklı türde kişiler vardır. Yine de, hepsini çözümün bir parçası haline

getirmenin bir yolu vardır. Onları pasifliklerinden kurtarmak, zorbalarla iş birliği yapmalarını engellemek. Örneğin, onları seyirci olmaktan vazgeçmeye davet etmek ilk adımdır, mağdura özel olarak destek göstermeleri ikinci adımdır, üçüncü adım ise daha yüksek bir katılım gerektiren, çevrimiçi zorbalık durumuna karşı aktif ve kamuoyuna açık bir tavır almaktır.

Sosyal ağ siteleri ve oyunlar gibi birçok çevrimiçi hizmetin, kullanıcılarının saldırgan davranışlarını yasaklayan kullanım politikaları vardır.

Dijital İlişkiler İçin Alanlarda İyi Bir Atmosferin Oluşturulmasına Değer Katmak

Çevrimiçi şiddet düzeyi o kadar yüksek ki, normalleşmemesi veya yaygın bir özellik olarak kabul edilmemesi için doğrudan karşı koyulması gerekiyor. Fark vurgulanmalı ve bunu yapmak için, akranlar arasında farkındalık yaratmak yoluyla, iyi bir çevrimiçi atmosferin ve saygı ve her türlü çeşitliliğe hoşgörü gibi temel değerlerin olumlu yönlerini vurgulamaktan daha iyi bir şey yoktur. İyi bir birlikte yaşama atmosferinin olumlu algılanması, şüphesiz, ona daha büyük bir bağlılığa ve onu yok eden eylemlerin reddedilmesine yol açar.

MÜDAHALE. SİBER ZORBALIK DURUMUNDA NE YAPILMALI?

Siber zorbalık durumunun kanıtına sahip olunması veya belirtilerinin farkında olunması durumunda harekete geçmek, çeşitli faktörlere bağlı olabilir (okul ve sosyal bağlam, zorbalığın derecesi ve süresi, mağdurların ve saldırganların profilleri gibi). Eğitim otoritelerinin veya okulun belirli bir protokolü olsa bile, her zaman dikkatli ve ihtiyatlı davranmanın yanı sıra bilinçli karar verme de göz önünde bulundurulmalıdır. Bu, gerçekleri veya durumu tespit etmenin, onu düzeltmek için gerekli eylemi gerçekleştirmek kadar zor olduğu kaygan bir zemindir. Ayrıca, zorbaların da yardıma ihtiyaç duyabilecek kişiler olabileceği akılda tutulmalıdır.

Siber Zorbalık Mağdurları İçin Uygulanabilir On Kural

Tüm siber zorbalık mağdurları, zorbalarından sadece bir tık uzaktadır. Uygun bir şekilde derhal harekete geçmek çok önemlidir. Bazen inisiyatif, mağdurun kendisinden gelir çünkü yardım bulamazlar veya örneğin yardım istemek istemezler. Eylemi kimin başlattığına bakılmaksızın, işbirliği çok önemlidir. Bu nedenle, öğretmenler doğrudan yardım sağlamaya çalışsalar da, mağdurun kendine de yardım edebilmesini sağlamalıdır. Bu on kural, zararını sınırlamak veya durdurmak için öğrencilere aktarılacak bir prosedür kılavuzu olabilir:

1. Yardım isteyin. Babanıza, annenize veya, bunlar mümkün değilse, güvendiğiniz bir yetişkine başvurun. Bu kişinin bu kuralları bildiğinden ve anladığından emin

olun, böylece ikiniz de aynı yönde kürek çekebilirsiniz ve sizi korumaya çalışırken istemeden zararı artırmazlar.

2. Asla provokasyonlara veya hakaretlere yanıt vermeyin. Bunu yapmak size hiçbir şekilde yardımcı olmaz. Aksine, bu sizi zorbalık yapanları cesaretlendirebilir ve onlara avantaj sağlayabilir. Sakin kalın ve asla dürtüsel veya abartılı bir şekilde davranmayın.

3. Varsayımlarda bulunmayın. Ne koşullar ne de ilgili kişiler göründükleri gibi olmayabilir. Makul şüphe payı bırakın, çünkü yanlış temelde hareket etmek sorunları daha da kötüleştirebilir ve yeni sorunlar yaratabilir.

4. Bu yerlerden uzak durmaya çalışın. Durum netleşene kadar, zorbalığa uğradığınız yerlerden mümkün olduğunca uzak durmaya çalışın. Bu sosyal ağlarda veya çevrimiçi topluluklarda oluyorsa, sizin için zor olmamalıdır.

5. Başkaları sizin hakkınızda ne kadar çok şey bilirse, o kadar savunmasız olursunuz ve size verebilecekleri zarar o kadar çeşitli ve yoğun olur. Gerçek özel verilerinize dayanan ve kolayca görülebilen bir yalanın sizi alaya aldığını hayal edebiliyor musunuz? Sizin gibi davranan biri arkadaşlarınızı aşağılarsa ne olurdu? Bu nedenle, tam olarak güvenmediğiniz kişilere çevrimiçi özel hayatınızın kapılarını kapatmanın zamanı geldi. Bunu şu şekilde yapabilirsiniz:

a. İzinsiz girişlerden kaçının. Bunu yapmak için, aşağıdaki adımları tam olarak bu sırayla tamamlamanız gerekir:

a.1. Sizi zorbalık yapan kişiye avantaj sağlayabilecek kötü amaçlı yazılımların (truva atları, kötü amaçlı yazılımlar vb.) olmadığından emin olmak için cihazlarınızı iyice kontrol edin.

a.2. Kullandığınız çevrimiçi hizmetlerin şifrelerini değiştirin, şifrelerin tahmin edilmesi zor ve sayı ve harfleri birleştirmesi gerektiğini unutmayın.

b. İletişim listenizi temizleyin. Sosyal ağlarınıza veya diğer çevrimiçi sosyal ortamlara eklediğiniz kişilerin listesini gözden geçirin ve azaltın.

c. Yeniden yapılandır. Kullandığınız sosyal ağların veya benzer sitelerin gizlilik ayarlarını yeniden yapılandırın ve sıkılaştırın. Bu seçeneklerin nasıl çalıştığının ve sonuçlarının tamamen farkında olduğunuzdan emin olun.

d. İnsanların sosyal medyada sizin hakkınızda neler söylediğini kontrol edin. Başkaları tarafından yayınlanan hakkınızdaki bilgileri arayın ve size zarar vermek için kullanılabileceğini düşünüyorsanız kaldırmaya çalışın.

e. Yayınladığınız bilgileri gözden geçirin. Yayınladığınız bilgileri ve bunlara kimlerin erişebileceğini gözden geçirin ve ayrıca bunları diğer kişilerin kullanımına sunun.

f. İletişim kurduğunuz kişilere bunu bildirin. Bilgilerinizin veya fotoğraflarınızın toplu ortamlarda yayılmasını istemediğinizi bildirin.

9. Kişisel verilerinizin korunması hakkınızı kullanın. Görüntünüz de dahil olmak üzere, bunların nasıl kullanılabileceğine siz karar verirsiniz.

6. Zorbalığa dair kanıtları saklayın. Zorbalığın kanıtlarını her zaman, hangi biçimde olursa olsun, saklayın. Bu size büyük ölçüde yardımcı olabilir. Ayrıca, herhangi bir kişinin haklarına zarar vermeden, yazarların kimliğini öğrenmeye veya güvence altına almaya çalışın.

7. Tacizcilerinize yaptıklarının sizi rahatsız ettiğini söyleyin ve agresif veya tehditkar olmadan durmalarını isteyin. İletişiminizde gerçekleri veya kişileri hafife almamanız gerektiğini unutmayın, bu nedenle bunu yaparken çok dikkatli olmalısınız. Kamuoyu önünde parmak sallamadan, ancak aynı zamanda ilgili kişi veya kişilerin mesajı aldığından emin olmaya çalışarak.

8. Zorbalıklarına devam ederlerse yaptıklarının kanunen cezalandırılabilirliğini onlara bildirmeye çalışın. Bir dava veya mahkumiyet hakkında çevrimiçi haberleri kontrol etmelerini önerebilirsiniz, böylece kendileri de görebilirler.

9. Önceki uyarınıza rağmen zorbalığa devam ederlerse, şikayette bulunmaya hazır olduğunuzu açıkça belirtin. Baştan beri yeterli kanıt topladığınızı ve nasıl ve nereye şikayet edeceğinizi bildiğinizi belirtin. Siber zorbalık devam ederse, savcılığa gitmekten başka seçeneğiniz kalmayacağını belirtmelisiniz.

10. Bu noktada zorbalık durumu hala devam ediyorsa, yasal işlem başlatın.

Bu önerileri uygulamaya koymak için aşağıdaki noktaları dikkate almak önemlidir:

- Bunlar çoğunlukla yetişkinlere ve okul dışı ortamlara uygulanabilir kılavuzlar olsa da, çocuklara ve ergenlere iletilirken mesaj uyarlanmalıdır.
- Her vaka ve her kişi farklıdır. Bu nedenle, bu tavsiyeler en yaygın durumlarda tamamen veya kısmen yardımcı olmak amacıyla hazırlanmıştır.
- Eylemlerin gerçekleştirilme sırası önemlidir. Bununla birlikte, bazı durumlarda olayların ciddiyeti, belirli adımların uygulanmasını hızlandırmayı, aralarındaki süreyi kısaltmayı veya tamamen atlamayı gerektirebilir.
- Aşırı durumlarda, savcılık yardımına hemen başvurulmalıdır.

Son olarak, mağdurun çevresiyle ilgili olarak üç temel ilke uygulanmalıdır:

1. Mağduru koruyun ve destekleyin. Bu en önemli şeydir. Kendini teselli edilmiş, anlaşılmış ve eşlik edilmiş hissetmelidir.

2. Tüm varsayımlardan vazgeçin, çünkü aldatma, zorbaların ve internetteki saldırganların en sık kullandığı araçlardan biridir.

3. Sakin ve soğukkanlı davranın, diğer tüm müdahale eden taraflarla işbirliği yapın. Mevcut şiddetin yoğunluğunu artırmak veya yaymak, hızlı bir çözüm bulmaya yardımcı olmayacaktır.



GiZLiLiK MAHREMiYET

Gizlilik - Mahremiyet

Gizlilik Neden Önemli

İki ana neden var:

Temel bir güvenlik unsurudur.

Kim olduğunuz, nasıl görüldüğünüz, arkadaşlarınız ve aileniz kimler, nerede olduğunuz, nelerden hoşlandığınız, ne yaptığınız vb. hakkındaki ayrıntılar, size zarar vermek isteyen biri için en iyi bilgi kaynağıdır.

Bu durum imajınızı, kimliğinizi ve dijital ayak izinizi etkiler.

Şu anda önemli olduğunu düşünmeyebilirsiniz. Yayınladığınız şeylerin veya sizin hakkınızda söylenenlerin sadece burada, şimdi ve düşündüğünüz kişiler için önemli olduğunu düşünebilirsiniz.

Ancak, internette sizin hakkınızda bilinenlerin bıraktığı iz, çok uzak olmayan bir gelecekte sizi olumsuz etkileyebilir. Bu iz derin, geniş ve silinmesi neredeyse imkansız olabilir.

Olası Olumsuz Sonuçlar Nelerdir?

Gizliliğinize gereken özeni göstermediğinizde, yayınlamak istediğiniz şeyleri ve kimlerin bunu bilebileceğini seçip yönetmediğinizde, belirli riskler yaratabilirsiniz:

- Çeşitli tehlikelere karşı daha savunmasızınız: cinsel siber yırtıcılar, siber zorbalık, şantaj, kimlik hırsızlığı vb.
- Kimliğiniz ve dijital itibarınız daha çeşitli ve yönetilmesi veya değiştirilmesi daha karmaşık hale gelir.
- Hayatınızın onlarla paylaştığınız anlarını yayınladığınızda başkalarını üzebilir veya onları riske atabilirsiniz.

UNUTMAYIN

- Eğer biri size zarar vermek istiyorsa, bunu birçok farklı yolla başarabilir ve sizin hakkınızda ne kadar çok şey biliyorlarsa, bu o kadar kolay olacaktır.
- Gizlilik ve siber güvenlik el ele gider. Cihazlarınız savunmasızsa veya şifreleriniz güvenli değilse, özel bilgileriniz risk altında olacaktır.
- Sizin hakkınızda bilinenler, diğer insanların eylemlerine de bağlıdır, tıpkı onların gizliliğinden sorumlu olduğunuz gibi.
- Gizliliğinizi korumak istiyorsanız, önleyici tedbirler almalısınız. Etkileşimde bulunduğunuz kişilere sizin hakkınızda ne tür bilgiler paylaşabileceklerini ve paylaşamayacaklarını ve nasıl paylaşabileceklerini söyleyin.

- Görüntünüz de dahil olmak üzere kişisel bilgilerinizin kullanımına karar verme hakkına sahipsiniz.
- Kullandığınız çevrimiçi hizmetler ve uygulamalar, farkında olmasanız bile, kişisel hayatınızı ifşa etmenin başka bir yoludur.

GİZLİLİK BİR HAK VE KORUMA FAKTÖRÜ OLARAK

Gizlilik artık bir seçenek değil. Gizlilik o kadar önemlidir ki, internetteki en önemli konulardan biri haline gelmiştir. Aslında, büyük internet şirketleri ve devlet kurumları arasında vatandaşlarının verilerini ve haklarını korumak için sürekli bir mücadele alanıdır. Ayrıca bireyler arasında da bir çekişme konusudur, çünkü internette sürekli olarak bilgi paylaşmaya davet ediliyor ve bazen de başkalarının bilgilerini paylaşmaya teşvik ediyoruz. Gizlilik, kum taneleri gibi parmaklarımızın arasından kayıp gidiyor.

Gizlilik Bir Hak Olarak

İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi zaten gizlilik hakkının bir insan hakkı olduğunu ortaya koymuştur. Bu makale, "Hiç kimse özel hayatına, ailesine, evine veya yazışmalarına keyfi müdahaleye veya şeref ve itibarına yönelik saldırılara maruz bırakılamaz. Herkes, bu tür müdahalelere veya saldırılara karşı hukukun korumasına sahip olma hakkına sahiptir" diyerek dijital çağda öz savunma hakkını da içermektedir.

Öte yandan, bu hak kapsamında, özel kırılganlık durumları nedeniyle çocuklar ve engelli kişiler için özel koruma önlemleri de bulunmaktadır.

Son olarak, Çocuk Hakları Sözleşmesi uyarınca "çocuğun en iyi menfaati", bir hak, hukuk ilkesi ve usul kuralı olarak kabul edilmelidir.

Koruma Faktörü Olarak Gizlilik

Şüphesiz ki, bir kişi hakkında ne kadar çok bilgi bilinirse, o kadar savunmasız hale gelir. Bu durum dijital bağlamda kritik önem taşır, çünkü bir kişiye zarar vermek çok kolay, anlık ve çoğu zaman cezasız kalır. İnternette mağdur ve saldırgan arasındaki güç dengesizliği, neredeyse her zaman zarar verenin lehine olan gizlilik faktörüyle artmaktadır. Saldırganlar kimliklerini gizlemek için anonimliğe, taklitçiliğe veya sahtekarlığa başvurabilirken, mağdurlar bunu yapamaz. Hâlâ kendi adlarıyla çevrimiçi yaşamlarını sürdürmek zorunda kalacaklar ve ne yazık ki, haklarında bilinenler konusunda tam bir kontrole sahip olmayacaklar.

Birine çevrimiçi olarak zarar vermek çok kolay (tehdit mesajları, iftira ve karalama, aldatmaca, karalama...) ve mağdur hakkında ne kadar çok bilgi bilinirse, o kadar çok zarar görürler.

Bu zararın yoğunluğu ve gizlenmesi ne kadar fazla olursa, o kadar da etkili ve gizli olabilir. Bu nedenle, daha güvenli bir internet için çalışmak, mağdur olma olasılığını ve olası zararın derecesini azaltmayı da gerektirir. Tüm bunlar, gizliliğin ve kişisel verilerin etkili ve bilinçli bir şekilde yönetilmesiyle bağlantılıdır.

GİZLİLİK KÜLTÜRÜNDE EĞİTİM

Vatandaşların gizlilik kaybı birçok farklı açıdan analiz edilebilir. Bu, kamu idareleri veya büyük şirketler arasında bilgi kontrolü, birleştirilmesi ve alışverişinden Nesnelerin İnterneti'ne (IoT) kadar uzanan oldukça geniş bir konu olduğundan, günlük normal sorunlara odaklanmak en iyisidir.

Gizlilik Yok Olma Tehlikesinde

Gizliliğimiz neden bu kadar azaldı? Basitçe söylemek gerekirse, bunun üretilen, depolanan, zenginleştirilen ve iletilen veya yayınlanan kişisel bilgilere bağlı olduğunu söyleyebiliriz.

- Daha fazla bilgi üretiliyor: Kişisel bilgilerin üretimi sürekli ve çoğu zaman bilinçsizdir. Hem paylaşılan ve etiketlenen kişisel bir görüntüyü (örneğin, cep telefonumuzun sürekli olarak kaydettiği coğrafi konum belirleme gibi) hem de bir ürün veya hizmetin elektronik olarak satın alınmasını düşünebiliriz. İlginç bir şekilde, hepimiz akıllı telefonumuza entegre edilmiş bir fotoğraf ve video kamera taşıyoruz.
- Daha fazla bilgi depolanıyor: Dijital bilginin depolanması, depolama birimlerinin fiyatlarının düşmesi ve daha çok yönlü hale gelen geniş teknoloji ve cihaz yelpazesiyle sürekli bir devrim geçirmiştir. Birkaç yıl içinde, cüzdanimızda bir akrabamızın basılı fotoğrafını taşımaktan, tanıdığımız ve hatta tanımadığımız kişilerin onlarca görüntüsünü ve videosunu cep telefonumuzda taşımaya geçtik.
- Daha zenginleştirilmiş bilgi: Bilgi yönetiminde, birbiriyle ilişkili veriler değerini katlar. Mevcut teknolojiler, bağlantılar, kanıtlar veya varsayımlar yoluyla yüksek katma değerli yeni türetilmiş bilgilerle sonuçlanan ve basitçe birleştirilmiş verilerin eklenmesinin ötesine geçen bilgileri kullanmamıza olanak tanır.
- Daha fazla bilgi iletiliyor/yayınlanıyor: Büyük şirketlerin veya kamu hizmetlerinin (yasalar ve öz düzenleme uygulamaları sınırları içinde) ne yaparsa yapsın, çoğu durumda bu bilgiyi paylaşmanın biz insanlar olduğumuz açıktır. Bunu yapmak daha kolay, daha uygun, daha hızlı ve daha ucuz hale geliyor ve biz de "hayatımızı paylaşmaya" davet eden ticari çıkarlara çok fazla dikkat ederek bunu abartıyoruz. Gizlilik yok olma tehlikesiyle karşı karşıya mı? Açıkçası, günümüzün gizliliği, cep telefonlarının yaygınlaşmasından önceki gizlilikle aynı değil.

Bu nedenle, günümüzün gizliliği, internetin evlerimize girmesinden önceki gizlilikle karşılaştırılmaz.

Öte yandan, kullanıcıları kişisel bilgilerin yaratıcısı ve tüketicisi olarak konumlandıran sosyal ağlar, gizlilik konusunda bir dönüm noktası oluşturdu. Bu durum, hayatımızı kolaylaştıran ve kelimenin tam anlamıyla attığımız her adımda hayatımızı dijitalleştiren akıllı telefonların normalleşmesiyle daha da belirginleşti.

İnternette Geleneksel Gizlilik Eğitimi

Nüfus arasında, özellikle de ergenler arasında farkındalık yaratmak amacıyla, kişisel verilerin korunmasına odaklanan iki yönü ele alan kampanyalar geliştirilmesi yaygın bir uygulama olmuştur. Bir yandan sosyal ağlardaki gizlilik ayarlarımızın yapılandırılması, diğer yandan ise kimlik ve dijital itibar. Her iki durumda da odak noktası, kişisel bilgilerin yayılmasını sınırlamak ve uzun vadede etkilerini düşündürmektir. Ayrıca, son zamanlarda, cep telefonlarının şifrelerle korunması ve başkaları hakkında yayınlanan bilgilerin onlara zarar verebileceği konusunda farkındalık yaratılması hakkında konuşmalar yapılmıştır. Bir bakıma, gizlilik yükünün kendimize düştüğü ve bunun tek eylem çerçevesi olduğu görülmektedir.

Ortak Gizlilik

Gizliliği kişisel bir mesele olarak ele almak, günümüz günlük yaşamımızdan çok uzaktır. Birbirine bağlı, aşırı bağlantılı insanların yaşadığı bir toplumda yaşıyoruz, burada varsayılan tutum, dürtü paylaşmaktır. Çocuklar ve ergenler bunu basitçe bir şaka veya bir hobi olarak görüyor. Ancak giderek artan sayıda genç ve yetişkin, bunu düşünmeden, ısrarla ve saplantılı bir şekilde yapıyor. Bu bazen "mahremiyetin ifşası", "aşırı paylaşım" veya "paylaşım" (ebeveynlerin çocuklarının resimlerini paylaşması) olarak adlandırılmıştır. Ancak, çoğu zaman, paylaşılan şey diğer insanların mahremiyetini de etkiliyor. Günümüzde, çevrimdışı hayatımızı paylaşmak, zorunlu olarak çevrimiçi olarak da paylaşmak anlamına geliyor ve bu noktadan itibaren mahremiyet çok hassas bir sorun haline geliyor. Bu nedenle mahremiyet artık sadece bize ait, tek başımıza kontrolümüz altında olan bir şey değil. Aksine, kolektif olarak yönetilen bir zenginlik, yani ortak mahremiyet haline geldi. Mahremiyet ve mahremiyetin değerini ve kültürünü teşvik etmek bu anlayış temelinde yapılmalıdır.

Özünde, ortak gizlilik, bireysel bir uygulama olmaktan ziyade, kendi gizliliğimizin, başkalarının gizliliğinin ve paylaşılan gizliliğin farkında ve sorumlu olduğumuz, üzerinde anlaşılmış bir uygulama olarak ele alınmalıdır. Elbette, hakkımızda neyin, nasıl ve nerede yayınlandığını bilmek önemlidir.

Ancak bunun kaynağı şüphesiz ki, diğer insanlara da bağlı olduğu için karar verme yeteneğimizin ötesindedir. Bu bağlamda, gizlilik, dijital vatandaşlık için haklar ve görevlerle ilgili bir uygulama haline gelir.

Siber Güvenlik ve Gizlilik

Gizlilik ve siber güvenlik arasındaki ilişki, kolektif bir konu olarak ele alındığında daha kolay anlaşılır. Bir yandan, gizlilik ve siber güvenlik birbirleriyle ilişkili kavramlardır, çünkü hiçbir bilginin güvenli ve emniyetli olduğundan emin olunmadıkça gizli kalacağı garanti edilemez. Öte yandan, siber güvenlik, topluluklar içinde yönetilmesi ve teşvik edilmesi gereken bir konudur. Bir ortam ne kadar güvenliyse, bileşenleri de o kadar güvenlidir. Birbirimize bağlı olarak yaşadığımız için, iyi bir siber güvenlik seviyesine ancak önceki temel prensipleri karşılayan bağlantılar varsa ulaşılabilir.

Kimlik ve Dijital Ayak İzi

Kimliğimiz ve dijital ayak izimiz, gizlilikle yakından ilgili ve büyük önem taşıyan iki unsurdur. Çünkü bunlar hem şimdi hem de gelecekte öğrencilerin sosyalleşmesini ve yaşamını etkileyebilir. Dijital kimliğimizin, internetin (veya genellikle Google ve daha az ölçüde Meta/Facebook, Instagram veya Twitter gibi diğer internet devleri olarak adlandırdığımız şeyin) insanların bizim hakkımızda düşüncelerini sağladığı şey olduğunu söyleyebiliriz.

Dijital ayak izimiz, her birimizin geride bıraktığı çevrimiçi izdir ve özellikle yaşamlarımız boyunca internette önemli bir etkiye sahip olan eylemlerle bağlantılıdır.

Öğrenciler bu iki kavramın öneminin ve onları nasıl etkilediğinin farkında olmalıdır. Her zaman böyle olmasa ve her zaman adil olmasa da, kimliklerinin dijital kısmı her geçen gün daha da önem kazanmaktadır. Uygunsuz çevrimiçi itibar veya eski bir yanlış davranışın kanıtı, insanların farkına bile varmadan veya bundan kaçınmadan olumsuz sonuçlar doğurabilir.

SOSYAL AĞLAR, ETİKETLEME VE COĞRAFİ KONUM BELİRLEME

Sosyal veya kültürel değişikliklerin yanı sıra, gizliliği ortadan kaldırmada iki unsur kilit rol oynamıştır. Bilgiyi sosyalleştiren sosyal ağlar ve otomatik olarak veri kaydeden cep telefonları, bunlar arasında coğrafi konum belirleme bilgileri de bulunmaktadır. Bu zorluğun bağlamında sorumlu ve proaktif bir şekilde hareket etmek için öğrenciler çok erken yaşlardan itibaren bunun farkında olmalıdır.

Sosyal Ağlarda Gizliliğin Yönetimi

Örneğin, gizlilik yönetimi sorusunu sosyal ağlar kapsamında sınırlandıırırsak, gizlilik üç faktöre bağlıdır:

- Kendimiz yayınladığımız şeyler ve bunu nasıl yaptığımız (kısıtlı, herkese açık...),
- Yayınladığımız platformun bu bilgiyi nasıl ele aldığı,
- Ve özellikle diğer insanlar.

Çok açıklayıcı bir örnek, sosyal ağlardaki resim etiketleridir. Resmi kimin yayınladığı önemli olmaksızın, birisi etiket ekleyerek fotoğrafta görünen her kişiyi sosyal ağdaki bir kimliğe bağlarsa, bunun çarpan etkisi olur. Sosyal platform, belirli kullanıcıların görüldüğü bir resmin yanı sıra, içinde yer alan tüm bilgileri de topluluğa bildirme sorumluluğunu üstlenir.

Bu, az ya da çok açık bir şekilde paylaşılabilir. Bu nedenle, gizliliği düzenleyen üç faktörden (ne yayımlandığı ve nasıl yayımlandığı, bu bilginin ve diğer insanların nasıl ele alındığı) en önemlilerinin yönetemediğimiz faktörler olduğu sonucuna varılabilir. İnsan, hangi platformda yayın yapacağımızı seçme ve bu bilgilerin mikro ve makro düzeylerde nasıl yönetildiğini bilme olanağına sahip olduğumuzu düşünebilir. Ancak gerçek çok farklı. Sosyal ağların değişen gizlilik kurallarının etkilerini kesin ve sürekli bir şekilde bilmeyi ne seçebiliriz ne de garanti edebiliriz. Sosyal medya görsellerindeki etiketler bunun açık bir örneğidir. Bu nedenle, öğrenciler arasında bu kadar yaygın bir konuyu gündeme getirmek iyi bir fikirdir.

Fotoğraf Etiketleri

İnternete görsel yüklemek her geçen gün daha kolay ve yaygın hale geliyor. Sosyal ağlar bağlamında, etiket ekleme, yani insanları bu görsellere bağlama olanağı da vardır. Öğrenciler bu işlevin sonuçları hakkında hiç düşündüler mi? Onlara bunları bulmalarına yardımcı olmalıyız.

Sosyal ağlardaki etiketler, gizliliğe karşı doğrudan ve açık bir saldırıdır. Çünkü platform, etiketlenen kişiden önceden ve açık izin istemelidir.

Kendi görüntüsünü paylaşarak ve kamuya açık hale getirerek.

Birinin, bir görüntüdeki ışık noktaları veya pikselleri kimliğinize atayarak sizi bir görüntüde (ve bağlam ve ek veriler açısından sonuçları) tanımlama hakkı nedir? Ve sosyal ağ bunu hangi etik gerekçelerle izin veriyor, teşvik ediyor ve yayıyor?

Bir sosyal ağda görüntü yayınlamak, ergenler için neredeyse günlük bir eylemdir. Çok sık olarak, bu görüntüler etiketlerle tamamlanır.

İnternete bir görüntü yüklemek, belirli durumlarda resimdeki kişilerin gizliliğine karşı bir saldırı olabilirken, etiketlerin kullanımı ne gibi bir etkiye sahip olabilir? Farklı sosyal ağlar arasındaki operasyonel ve yapılandırma farklılıklarını bir kenara bırakarak, genel olarak bir göz atalım. Basitçe söylemek gerekirse, bir görüntüdeki etiket, görüntüyü ve özellikle dikdörtgen bir alanını belirli bir kişiye bağlayan bir işaret veya semboldür. Bu işaret genellikle resimde bu kişinin bulunduğu alanla ilişkilendirilir. Etiketlendiğinizde ne olur? İki etkisi vardır:

- **İlişkilendirme etkisi:** Etiketlendiğinizde, bu görüntüye ve özellikle de genellikle sizin bulunduğunuz alana bağlanıyorsunuz. Ancak, bu ilişkilendirmeyi garanti etmenin bir yolu yoktur, çünkü sosyal ağ, yorumlayamadığı bir grafik alanı, bir piksel kümesi işaretlemenize olanak tanır.

- **Yayılma etkisi:** Etiketlendiğinizde, sosyal ağınızdaki "arkadaşlarınız" yeni bir resimde etiketlendiğiniz konusunda bilgilendirilir ve resmi görmek için tıklamaları yeterlidir. Sosyal ağların sunduğu, resimlerle bağlantılı bu işlevin çekim ve yayılma etkisi o kadar güçlüdür ki, kullanıcılar bunu orijinal amacından çok uzak olan bir resimdeki kişiyi tanımlamak gibi başka amaçlar için bile kullanırlar.

Kısacası, bu, diğer kişilerin bir resme bağlandığınız konusunda bir bildirim alacağı ve bu resmin yayınlandığını bilmeden önce bile görebilecekleri anlamına gelir. Şanslıysanız, bu resmin var olduğunu ve sizin de bir parçası olduğunuzu bilebilirsiniz. Hatta, hoşunuza gitsin ya da gitmesin, birinin bunu çevrimiçi olarak yüklemiş olabileceğini varsayabilirsiniz. Ancak etiket, diğer insanların ve sosyal ağların hayatınızın "habercisi" olarak yaptığı işin bir uyarısı, bir hoparlördür. Birdenbire, birçok "arkadaşınız" hayatınızın bir film karesini görebildiklerini ve çok sık olarak bunu başkalarıyla paylaşabildiklerini öğrenir.

Daha pratik bir düzeyde, ilgili kişisel veri mevzuatında ne belirlenmiş olursa olsun, etiketlerin gizlilik sorunlarına neden olduğu ve çoğu zaman kötü bir dijital birlikteliğin nedeni ve/veya sonucu olan belirli durumları belirleyebiliriz. Bunlardan bazıları kazara veya kasıtlı olarak meydana gelebilir:

- Davranış, yer, zaman veya şirket nedeniyle uygunsuz bir bağlamda etiketleme yapmak.
- Birinin fiziksel görünümünü sosyal ağda resimsiz veya avatarla gösteren etiketleme.
- Örneğin, etiketlenen kişinin kişisel imajına zarar veren veya tehdit edici nitelikteki bir fotoğrafla etiketlenmesiyle ilgili hakaretler, kamuoyu önünde yapılan tacizler ve tehditler.
- Söz konusu, incitici veya hoş olmayan görüntünün, etiketlenen kişi tarafından, kendisiyle ilgili bir etiket bildirimi üzerine görülmesini sağlayacak aldatma.

Coğrafi Konum Belirleme

Akıllı telefonlarda bulunan coğrafi konum belirleme veya coğrafi referanslama özelliği sayesinde, yani bulundukları yeri belirleyebilme özelliği sayesinde, daha fazla avantajdan yararlanabiliriz. Telefonların harita ve pusula olarak çalışmasıyla birlikte, bu özellikler, yakınlarda kimlerin olabileceği veya bu belirli yer ve zamanda hangi bilgilerin daha yararlı olabileceği gibi diğer ilgili verileri sağlar. Bu, gizlilik açısından bedel ödeyebilecek kullanıcılara büyük bir katma değer sunar.

İzinler açık modda ayarlanmışsa, cep telefonumuz ve uygulamalarıyla gerçekleştirilen herhangi bir işlem, elde edildiği konumu ve dolayısıyla o anda terminali kullanan kişinin konumunu (meta veri biçiminde, ilk bakışta fark edilmeyen veya daha açık bir şekilde) ek bilgi olarak taşıyabilir. Bunu yönetmek her zaman kolay değildir. Bu veriler, bir kişinin tam konumunu, coğrafi koordinatları da dahil olmak üzere veya bir fotoğrafın çekildiği yeri ortaya çıkarabileceği için güvenlik tehdidi oluşturabilir.

İzinler açık modda ayarlanmışsa, cep telefonumuz ve uygulamalarıyla gerçekleştirilen herhangi bir işlem, elde edildiği konumu ve dolayısıyla o anda terminali kullanan kişinin konumunu (meta veri biçiminde, ilk bakışta fark edilmeyen veya daha açık bir şekilde) ek bilgi olarak taşıyabilir. Bunu yönetmek her zaman kolay değildir. Bu veriler, bir kişinin tam konumunu, coğrafi koordinatları da dahil olmak üzere veya bir fotoğrafın çekildiği yeri ortaya çıkarabileceği için güvenlik tehdidi oluşturabilir.

Bu konuda farkındalık yaratılmalıdır. Yüklenen uygulamalar varsayılan olarak konum belirleme modunda ayarlanmıştır. Telefonun yazılımı, her zaman ve ilk fırsatta, terminaldeki konum verilerine erişim izni vermemizi isteyecektir. Bunu, farkında bile olmadan kaçırılma gibi ciddi tehlikelere maruz kalabilecek çocuklar ve ergenler için vurgulamalıyız.

GİZLİLİK BİR HAK VE KORUMA FAKTÖRÜ OLARAK

Akıllı telefonunuz çok miktarda bilgi ve kişisel veri barındırıyor. Kişileriniz, Instagram veya WhatsApp gibi genellikle kullandığınız uygulamalara erişiminiz, fotoğraflarınız vb. hepsi cep telefonunuzda bulunuyor. Telefonunuzda ayrıca, farkında olmayabileceğiniz başka bilgiler de saklanıyor. Bağlandığınız WiFi ağları veya bulunduğunuz yerler.

Bu nedenle, okul çocuklarının bu konunun tamamen farkında olmaları ve cep telefonlarının kullanımının bu konuda bir tehdit oluşturmaması için ellerinden

gelen tüm önlemleri uygulamaları gerekiyor. Aşağıda, farkında olunması, anlaşılması ve kabul edilmesi gereken on öneri bulunmaktadır.

Cep Telefonunuzun Gizliliğini Korumak İçin On Kural

1. Cep telefonunuzdaki kötü amaçlı yazılımlarla mücadele etmek için güvenlik yazılımı (antivirüs) yükleyin.
2. Güvenliğinizi artırmak için cep telefonunuzdaki işletim sistemini güncel tutun.
3. Cihazınızı güçlü bir şifre (rakamlar ve harfler) veya desenle koruyun.
4. Şifrenizi sizin için daha önemli olan uygulamalarda saklamaktan kaçının.
5. Kaybetmeniz durumunda cep telefonunuzun konum servisini etkinleştirin.
6. Kaybolması veya çalınması durumunda cep telefonunuzdaki verileri uzaktan nasıl bloke edeceğinizi ve sileceğinizi öğrenin.
7. Yalnızca ihtiyaç duyduğunuzda ve sonuçlarının farkında olarak, cihazda ve bireysel uygulamalarda coğrafi konum belirlemeyi etkinleştirin.
8. Her uygulamayı yüklerken istenen yetkilendirmeleri doğrulayın ve kötüye kullanım içermediklerinden emin olun.
9. Kötü amaçlı yazılımlardan kaçınmak için uygulamalarınızı resmi mağazalardan yükleyin.
10. Bilinmeyen bağlantıları, dosyaları veya bilinmeyen Wi-Fi ağlarını açmadan önce özellikle dikkatli olun.

ÖZEL HAYATINIZI VE VERİLERİNİZİ GÜVENDE TUTMANIN ANAHTARLARI

Gizlilikten bahsederken, siber güvenlikten ve dolayısıyla öğrencilerin, çocukların ve gençlerin sağlığı ve refahından bahsediyoruz. Bu konuda yetkin, bilinçli ve eleştirel bireyler olmalarına yardımcı olmak ve onlara aşağıdaki temel yönergeleri sağlamak çok önemlidir:

- Cihazlarınızın ve internet bağlantılarınızın güvenliğine dikkat edin.
- Güçlü şifreler kullanın.
- Bilgisayarınızı kullanmadığınız zamanlarda kamerasını kapatın.
- Ekranda görünen her şeyin kaydedilebileceğini unutmayın: konuşmalar, resimler, videolar... O andan itibaren, bunlar üzerindeki kontrolünüzü sonsuza dek kaybedersiniz.
- Coğrafi konum gibi meta verileri (ek gizli veriler) dikkate alın. Bu, bilginiz olmadan sizin hakkınızda birçok şeyi ortaya çıkarabilir.
- Cihazlarınızdaki, uygulamalarınızdaki ve sosyal ağlarınızdaki gizlilik ayarlarına özellikle dikkat edin:

- İlgili seçeneklerin nerede olduğunu öğrenin.
- Anlamalarını ve sonuçlarını anladığınızdan emin olun.
- Tercihlerinize ve ihtiyaçlarınıza göre bunları etkinleştirin.
- Bunlarda herhangi bir değişiklik olmadan önce tetikte olun.
- Gizliliklerini kötü yöneten veya temel siber güvenlik önlemlerini almayan kişilere karşı dikkatli olun, çünkü bu sizin için olumsuz sonuçlar doğurabilir. Onlara yardım ederek kendinize de yardım etmiş olursunuz.
- Sosyal ağlarda görselleri etiketlemekten kaçının, çünkü kişilerle bağlantılı görseller çok fazla bilgi sağlayabilir.



İnternetteki
Dezenformasyon
ve Yanlış
Bilgilendirme

İnternetteki Dezenformasyon ve Yanlış Bilgilendirme

İnsanları medya ve bilgi okuryazarlığı yoluyla güçlendirmek, bilgiye ve bilgiye eşit erişimi teşvik etmek ve özgür, bağımsız ve çoğulcu medya ve bilgi sistemlerini desteklemek için en önemli gereksinimlerden biridir.

Küresel, telaşlı ve birbirine bağlı dijital bir toplumda içeriğin oluşturulma kolaylığı ve çoğaltılma ve viral hale gelme hızı, "bilgi bozuklukları" (dezenformasyon ve yanlış bilgilendirme) olarak adlandırılan durumlara yol açmıştır ve tetikleyebilecekleri ciddi sonuçlar nedeniyle endişe verici bir konudur.

Özetle, kasıtlı veya kasıtsız olarak oluşturulan hatalı içerik ve bilgileri tespit etmek, ifşa etmek ve genel olarak bunlarla mücadele etmek hem kişisel bir meydan okuma hem de kolektif bir ihtiyaç haline gelmiştir diyebiliriz.

UNUTMAYIN

Bilgi bombardımanının giderek arttığı, düzensiz ve farkında olmadığımız çıkarlar tarafından yönlendirilen bir dönemde yaşıyoruz. Dezenformasyon oluşturmak otomatikleşmiştir. Bunun kanıtı, gerçek gibi görünen sahte bir içerik oluşturma imkanı sunan web sitelerinin varlığıdır. Bu bağlamda, sorumlu siber vatandaşlık, katılım odaklı ve gerçek bilgilere dayalı olarak, dezenformasyonun yayılmasına karşı mücadeleci bir duruş sergileyerek uygulanmalıdır.

Etik vatandaşlık açısından, dezenformasyonun şu etkileri olduğunu hatırlamak önemlidir:

- Belirsizlik ve kafa karışıklığı yaratmak, ayırt etmeyi ve pozisyon almayı zorlaştırmak.
- Kişisel kararları doğrudan veya dolaylı olarak manipüle etmek.
- Kişilerin, şirketlerin veya kurumların itibarını zedelemek veya itibarsızlaştırmak, onlar hakkındaki algıyı ve görüşü manipüle ederek.
- Finansal kareelde etmek.
- Kamuoyunu, belirli ideoloji türlerine veya çıkar gruplarına fayda sağlayabilecek bir görüş durumu yaratacak şekilde şartlandırmak.

Kişisel açıdan, dezenformasyonun etkisi altındakiler:

- Zamanlarını boşa harcarlar ve faydasız bir şekilde dikkatleri dağılır.
- Manipüle edilebilirler ve sonuç olarak hareket etmeyebilir veya özgür bir görüşe

sahip olmayabilirler. Ayrıca yanlış hareket edebilirler.

- Bilmeden bir yayım zincirinin halkası haline gelebilirler.
- Başkalarını olumsuz etkileyen dezenformasyonun yayılmasına katılmaktan kaynaklanan sonuçlara, hatta yasal sonuçlara bile katlanabilirler.

Dezenformasyonla mücadele doğrudan her bireyin yeteneklerine bağlıdır. Bu mücadele bilmekle, ama özellikle gördüklerimizi veya okuduklarımızı sorgulamakla ilgilidir. Bu, basit bir görme veya duyma eylemi olmaktan ziyade, dikkatlice gözlemlene ve dinleme görevidir.

TANIM, KAVRAMLAR VE ÖZELLİKLER

Dezenformasyon ve Yanlış Bilgi

"Bilgi Bozukluğu:

- Dezenformasyon. Bir kişiye, sosyal gruba, kuruluşa veya ülkeye zarar vermek amacıyla kasıtlı olarak oluşturulan yanlış bilgi.
- Yanlış bilgi. Yanlış olan ancak zarar verme niyetiyle oluşturulmamış bilgi.

Ayrıca, bilginin kötü amaçlı kullanımı, gerçekliğe gevşek bir şekilde dayanan ancak bir kişiye, kuruluşa veya gruba zarar vermek için kullanılan bilgiyi de ifade edebilir.

Bu bağlamda, yukarıda belirtilen tanımların anlamını ve kapsamını tamamlamaya ve anlamaya yardımcı olan bazı hususların açıklığa kavuşturulması gerekmektedir:

- Dezenformasyon genellikle planlanır, organize edilir ve zararlı bir amaca ulaşmak için gerekli araçlara sahiptir.
- Yanlış bilgilendirme vakalarında, zararlı bir niyete sahip olmamalarının yanı sıra, bunu yayanların genellikle bunun yanlış bilgi olduğunun farkında olmadıkları belirtilmelidir.
- Bilginin kötü amaçlı kullanımının bir özelliği, etik olmayan amaçlar için kullanılmasıdır.

Son olarak, yanlış haberlere atıfta bulunmak için "sahte haber" teriminin kullanılması hiçbir şekilde tavsiye edilmez, çünkü bu, haber olmayan bir şeye haber statüsü kazandırır.

Belirli bir yanlış bilgi türünü üretebilecek çeşitli kaynaklar ve stratejiler vardır:

- Hiciv ve parodi.
- Tıklama elde etmek için tasarlanmış başlıklar (tıklama tuzağı başlıkları).
- Altyazıların, görsel kaynakların veya istatistiklerin aldatıcı kullanımı.
- Bağlamından koparılmış gerçek içerik paylaşımı.

- Sahte içerik (ilgili olmayan gazetecilerin isimleri veya medya logoları kullanıldığında).
- Manipüle edilmiş ve uydurulmuş içerik.

MEDYA VE BİLGİ OKURYAZARLIĞI

Medya ve Bilgi Okuryazarlığı,

"Anlama, Eleştirel Düşünme, Yaratıcılık, Kültürlerarası Bilinç ve Vatandaşlık" olarak tanımlanan beş temel beceriye odaklanır.

ELEŞTİREL DÜŞÜNME, BECERİLER VE TUTUMLAR

Eleştirel düşünme, Dünya Sağlık Örgütü (WHO) tarafından "bireylerin günlük yaşamın talepleri ve zorluklarıyla etkili bir şekilde başa çıkmalarını sağlayan uyarlanabilir ve olumlu davranış yetenekleri" olarak tanımlanan Yaşam Becerilerinden biridir.

Eleştirel düşünme, iyiyi kötüden, adil olanı haksız olandan ayırmaya veya doğruyu yanlıştan ayırt etmeye yardımcı olur. İlk etapta, eleştirel düşünme, kendimizle pratik yaparak geliştirilebilir. Mantıksal argümanlar ve sorgulama yoluyla önyargıları, önceden belirlenmiş fikirleri ve bilişsel önyargıları ortadan kaldırmak temel önemdedir.

Eleştirel düşünme şunları içerir:

- Geniş bir konu yelpazesine karşı merak.
- İyi bilgilendirilmiş bir kişi olma ve kalma kaygısı.
- Eleştirel düşünmeyi kullanma fırsatlarına karşı uyanıklık.
- Mantıklı sorgulama süreçlerine güven.
- Kendi akıl yürütme yeteneğine olan özgüven.
- Dünyaya ilişkin farklı görüşlere açık fikirlilik.
- Alternatifleri ve görüşleri değerlendirirken esneklik.
- Başkalarının görüşlerini anlama.
- Değerlendirmede adalet.
- Kendi taraflılığını, önyargısını, kalıplaşmış düşüncelerini veya bencil eğilimini tanıma ve dürüstçe yüzleşme.
- Yargıları askıya alma, verme veya değiştirme konusunda ihtiyatlılık.
- Dürüst bir öz yansıtma, değişimin haklı olduğunu gösterdiğinde bakış açılarını yeniden değerlendirme ve gözden geçirme isteği.

Prosedürel bir bakış açısından yaklaşıldığında, eleştirel düşünme en az beş temeleylemi içerir:

- Anlamını açıklığa kavuşturmak için bilgiyi yorumlamak.
- Kaynak, tutarlılık ve kasıtlılık veya olası etkilerin yanı sıra kişinin önceki bilgisine dayanarak bilginin güvenilirliğini doğrulamak.
- Açık ve örtük verileri ve bilgileri sorgulamak ve alternatifler tanımlayarak bunları karşılaştırmak.
- Daha fazla veri elde ederek, ancak aynı zamanda bilinmeyen gerçekleri belirleyerek daha fazla içgörü kazanmak.
- Kendi zihinsel sürecini gözden geçirerek, ardından elde edilen akıl yürütmeyi ve nihai sonuçları sorgulamak, doğrulamak veya gözden geçirmek için bilgi edinerek öz değerlendirme yapmak.

Bu eylemlerin sonucunun kişinin entelektüel yeteneğiyle ne ölçüde ilişkili olduğu sorgulanmaya değerdir. Zeka (ölçülebilir bir zeka katsayısı (IQ) düzeyi olarak anlaşılan) ile eleştirel düşünme arasında mantıksal bir ilişki olduğu söylenebilir. Bu ilişki açık görünmektedir, çünkü bilgiyi doğru değerlendirmek, onu elde etmeyi, işlemeyi ve anlamayı gerektirir ve en yüksek IQ'ya sahip kişiler bilişsel önyargılara karşı daha dirençlidir. Bununla birlikte, eleştirel düşünme, zeka testleri veya kişilik özellikleri ile ölçülemeyen diğer bilişsel yeteneklere de bağlıdır.

Eleştirel düşünmeyi teşvik eden insanların üç özelliği:

- Açık keşfi teşvik eden merak veya açıklık
- Gerçeği bulma arzusu, çabaya girişmek için bir motivasyon görevi görür.
- Entelektüel alçakgönüllülük, eleştirel düşünmenin diğer insanları, ama her şeyden önce kendini sorgulamayı gerektirdiği için hayati önem taşır. Eleştirel düşünme, bilgi eksikliğini varsayarak başlayan bir tutumdur.

Eleştirel düşünmeyi geliştirmek, araştırmalara ve çalışmalara göre, yaşamın diğer alanlarında şu avantajları sağlayan üst düzey akıl yürütme yeteneklerini teşvik etmek anlamına gelir:

- Daha iyi kararlar alınmasını teşvik etmek.
- Olumsuz olayların sıklığını azaltmak.
- Akademik performansı iyileştirmek.
- Analitik beceriler gerektiren faaliyetlerde verimliliği artırmak.

Sonuç olarak, eleştirel düşünmeyi geliştirmek ve etkinleştirmek, yalnızca dezenformasyon ve yanlış bilgilendirmenin dayattığı bir ihtiyaç değil, aynı zamanda kişinin kendi kişisel ve profesyonel yaşamını iyileştirme fırsatıdır.

ERGENLİK DÖNEMİNDE DİJİTAL YAŞAM VE ELEŞTİREL DÜŞÜNME

Ergenlik döneminde eleştirel düşünme, özellikle dijital yaşamları için temel öneme sahiptir. İnternet, aldatmaya yatkın özelliklere sahip bir ortamdır, sahtekarlığa çok açıktır ve aynı zamanda nicelik ve hızın çoğu zaman nitelik veya doğruluğun önüne geçtiği bir yerdir.

Erken yaşlarda eleştirel düşünmeyi kullanmak, sosyal sorumluluk meselesi olmasının yanı sıra, güvenlik ve refah için de bir araçtır. Örneğin, erkekler, kızlar ve ergenler, sağlıkla ilgili yanlış bilgilendirme veya dezenformasyon (yeme bozuklukları, mucize diyetler vb.) tüketildiğinde risk altındadır. Doğrulanmamış veya çapraz kontrol edilmemiş yeni çevrimiçi hizmetlere erişirken veya bunları kullanırken sorun yaşayabilirler. Öte yandan, çocuklar ve ergenler ne yaptıklarını, neden yaptıklarını ve bundan gerçekten kimin en çok fayda sağlayacağını sorgularlarsa, dijital tüketimlerini kötüye kullanıma düşmeden daha iyi yönetebilirler.

YANLIŞ BİLGİDE ÖNYARGI, DUYGULAR VE ÖNEMLERİ

Yanlış bilgi birçok biçim alabilir. Bunların hepsinin aynı amacı olmasa da, bazıları etkili olmak için stratejileri paylaşabilir. Biz, insanlar, ekranın bu tarafındayız ve yanlış bilgi, ona nasıl tepki verdiğimizize bağlı olarak azya da çok başarılı olacaktır.

Bir şeye verdiğimiz tepki beynimizden ve kalbimizden geçer. Akıl yürütmemiz ve duygularımızdan süzülür. Bilginin bu mantıklı yorumlanması bazen bilinçsizce gerçekleşir ve bilişsel önyargılardan etkilenebilir.

Bilişsel önyargı, düşüncelerin işlenme biçimini, yargıların verilmesini ve kararların alınmasını etkileyen, mevcut bilgilerin sistematik olarak hatalı yorumlanmasıdır. Bilişsel önyargılar çeşitli kaynaklardan gelir: kültür, sosyal etkiler, duygusal veya etik motivasyonlar, bilgi işleme süreçlerinin basitleştirilmesi, hafıza vb.

Önyargılar, beynimizin sorunları basitleştirmek ve kararları kolaylaştırmak için geliştirdiği kısa yollardır. Önyargılar, uyarınları seçici olarak filtrelemek için evrimsel bir ihtiyacın sonucudur ve beyni bilgi analizi görevlerinin bir kısmından kurtarır. Bununla birlikte, genellikle yanlış bilgiyi tespit etmede bir engeldirler. En yaygın önyargılardan bazılarına bakalım:

- En büyük önyargı kör nokta olarak adlandırılır. Bu önyargı, diğer insanların önyargılarını fark ettiğimiz ancak kendi önyargılarımızın farkında olmadığımız veya zorluk çektiğimiz duruma uygulanır.

- Onaylama önyargısı, kendi inançlarımızla (değerlerimiz, ideolojilerimiz, önyargılarımız) örtüşen bilgileri aşırı değerlendirmemize veya bu başarısız olursa, baskın inançlarımıza yönelmemize ve kendi görüşlerimiz ile uyuşmayanları bilinçsizce görmezden gelmemize yol açar.
- Ters etki yaratan aşinalık önyargısı şunlardan oluşur: Belirli bilgilere (doğruluğundan bağımsız olarak) ne kadar sık maruz kalırsak, onu doğru olarak kabul etme olasılığımız o kadar artar.
- Sosyal etkileşim önyargısı, diğer insanların yaptıklarını yapmamıza yol açarak, bir gruba ait olma duygusu gibi temel bir şeyi güçlendirir.
- Görsel üstünlük etkisi, beynimizin bir görüntüyü yazılı metinden 60.000 kat daha hızlı işlemesinden kaynaklanır. Öte yandan, gördüklerimizin %80'ini, okuduklarımızın %20'sini ve duyduklarımızın %1'ini hatırlarız. Görsellerle desteklenen içerik, görsel içermeyen içeriğe göre %84 daha fazla ziyaret alır ve 40 kat daha fazla paylaşılr.
- Güdüsel akıl yürütme duygusal önyargıdır: Bilgi işlemeyi bilinçsizce belirli bir amaca veya hedefe ulaşacak şekilde koşullandırma eğilimimiz.
- Kullanılabilirlik önyargısı, bir olayın olasılığının, bu olayın örneklerinin aklımıza gelme kolaylığıyla belirlendiği bilişsel sezgisel yöntemleri ima eder. Bu, insanların yanlış bir ifadeyi doğru olarak algılamasına neden olabilir, çünkü onu kolayca hatırlayabilirler.

Duygular da dezenformasyonla mücadelede yardımcı olmaz, çünkü düşünme sürecimiz rasyonel olduğu kadar duygusaldır da. Bilgi belirli bir duyguyu tetiklediğinde, bu, önceki bilginin analizini rasyonel bir gerekçelendirmeye dönüştürebilir.

Bazı duyguları yönetmek özellikle zordur ve kontrolümüzü kaybetmemize neden olur. Bunlar arasında öfke, şefkat, hayranlık, merak, korku ve aciliyet yer alır. Dezenformasyon bunları besler ve düşünme sürecimizin duygusal bileşeni nedeniyle onu paylaşmamızı teşvik eder.

FİLTRE BALONU VE YANKI ODALARI

Filtre balonu kavramı, internetin (arama motorları, sosyal ağlar, eğlence sağlayıcıları, çevrimiçi mağazalar vb.) bize sunduğu bilgilerin kendi özelliklerimizle sınırlı olduğu gerçeğine işaret eder. Teknoloji, bilgiyi bize, muhtemelen bizim için sahip olacağı alaka düzeyine veya önemine göre sunulacak şekilde uyarlamamıza olanak tanır.

Sosyal medya ve dijital platformlarda karşımıza çıkan filtre balonu ve yankı odaları, algoritmaların yalnızca duymak istediklerimizi bize sunarak bizi kendi fikirlerimizin oluşturduğu kapalı bir döngüde hapsedme durumudur.

Yanlış bilgilendirmeye mücadele etmek için bunun farkında olmalıyız, çünkü eleştirel düşünme sadece açık ve ulaşılabilir olanı değil, aynı zamanda önümüzde görünmeyebilecek olanı da kapsamalıdır. Bu tür filtre baloncukları, keşfetme yeteneğimizi ve merakımızın sonuçlarını, ayrıca sorgulama veya daha derine inme fırsatını sınırlar. Eleştirel düşünmenin önünde bir engeldirler ve dolayısıyla yanlış bilgilendirmenin müttefikleridir.

Medya tüketimiyle ilgili olarak, yankı odaları teorisi, insanların benzer insanlara ve bilgilere yönelik bir tercih göstermeleri durumunda, bu yankı odalarının, yani kendi fikirlerimizin sekip geri döndüğü boş alanların oluşacağını belirtir.

Bu teori, dijital teknolojilerin seçimlerimizi genişletmediğini, aksine bu odalarda çalışarak olanaklarımızı sınırladığını ima eder. Belki bunun farkında değiliz ve kaynaklarımızı başlangıçta çelişkili olan etkiler ve fikirlerle bile zenginleştirmek için mekanizmaları çoğu zaman harekete geçirmiyoruz.

Kısacası, iyi durumda olduğumuza ve bu şekilde daha kolay, daha uygun ve daha hızlı olduğuna inanıyoruz. Bunu yaparak, eleştirel düşünme ve bireysel katkılar yoluyla kolektif yapıda yer almayı bırakıyoruz. Hem dijital hem de gerçek dünyada düşündüğümüz kadar özgür olup olmadığımızı düşünmeliyiz.

DEZENFORMASYONU ÖNLEMEK VE ONUNLA MÜCADELE ETMEK İÇİN NELER YAPILABİLİR?

Yukarıda belirtildiği gibi, eleştirel ve aktif bir nesli yanlış bilgilendirmeye karşı eğitmek için çeşitli müdahale yolları vardır.

DÜŞÜNMEK VE PAYLAŞMAMA SEÇENEĞİNİ DEĞERLENDİRMEK

Bilgi paylaşmak, açıkça söylenmediği veya aksi yönde motive edilmediği sürece, varsayılan bir davranış gibi görünür. Bunu düşünmek ve doğrulamadan paylaşmanın bir cömertlik eylemi değil, aksine destekleyici olmayan bir şey olduğunun farkına varmak gerekir. Yeterli doğrulama süresi harcamadan hiçbir şey paylaşılmamalıdır. Alınan bilginin yeterince güçlü bir şekilde doğrulanması için zamanınız, isteğiniz veya yeteneğiniz yoksa, tek sorumlu alternatif paylaşmamaktır.

Aşağıda, önceden doğrulama yapmadan paylaşmaktan kaçınmak için beş nedenin kısabir önerisi bulunmaktadır:

- Bilgiyi zorlayıcı veya aceleci bir şekilde paylaşırsanız, doğru olmama olasılığı daha yüksektir. Yaymanın önemli olduğunu düşünüyorsanız, doğruluğunu kontrol etmek için gerekli zamanı ayırmanız da önemlidir.
- Yanlış bilgi genellikle diğer insanlara veya çıkarlara zarar verir. Bunu yayarak katılırsanız, etkilerinden de sorumlu olursunuz.
- Katılım, görüş bildirme, fikirleri savunma, diğer insanlara yardım etme vb. vatandaşın hakkı ve görevidir. Ancak doğrulanmamış bilgilerin yayılması pervasız ve etik dışıdır.
- Bilmeden yanlış bilgi paylaştığınızda, hem mağdur olursunuz hem de onu yaratanların farkında olmadan suç ortağı olursunuz. Dahası, buna katılarak başkalarını da suçlayabilir ve onlara zarar verebilirsiniz.
- İfade özgürlüğü veya başkalarının yaydıklarını tekrarlamak, yanlış bilgi yaymaktan kaynaklanabilecek yasal sorumluluktan sizi muaf tutmaz. Son olarak, bilgi yayılmışsa ve yanlış olduğu tespit edilirse, bunu reddetmek ve yanlışlığı telafi etmeye çalışmak için bazı gerekli adımların atılması gerektiğini hatırlamak önemlidir.

ETKİLERİN FARKINDALIĞI VE KİŞİSEL SORUMLULUK

Yanlış bilgilendirmenin başkaları için olumsuz sonuçları vardır. Ne tür, nasıl veya kime zarar verildiğini bilsek de bilmesek de, zarar verilir. Ayrıca, daha önce de belirtildiği gibi, bu bilgi bozukluklarının etkilerinin az ya da çok gizli kurbanları oluruz. Bu nedenle, yanlış bilgilendirmeyi engellemek için soyut ve uzak kavramlar hakkında düşünmek kadar somut ve yakın kavramlar hakkında da düşünmek faydalıdır. Olumsuz sonuçları ve bu sonuçlardaki sorumluluğumuzu görselleştirmek, bulmak, bilerek veya bilmeyerek yanlış bilgilendirme zincirlerine katılımımızı önlemeye yardımcı olmalıdır.

Çoğu zaman odak noktası, erken yaşta bunu yapma becerilerini kazandırarak aldatmacaları ve yanlış bilgilendirmeyi tespit etmek ve bunlarla mücadele etmektir. Ancak belki de daha önemlisi, bu eleştirel ve sorumlu tutumu başlatmak için motivasyon sağlamaya, farkındalığı artırmaya ve nedenler sunmaya odaklanmaktır. Bunu nasıl yapacağını bilmek yeterli değildir, bunu yapmak istemek ve yeterli motivasyona sahip olmak gerekir.

GENİŞ ANLAMDA ELEŞTİREL DÜŞÜNMEYİ TEŞVİK ETMEK

Bilgiyi analiz etme ve değerlendirme (çıkarım ve sonuç) yeteneğini geliştirmenin ötesinde, öğrencilerin kendilerini ve yaklaşımlarını sorgulamalarına yardımcı

olacak etkinlikler sunmak önemlidir, böylece aceleci ve öfkeli bir şekilde görüşlerini veya yargılarını ifade etmelerini sınırlamayı öğrenirler.

Genellikle, rasyonel bir şekilde düşündüklerinin tam tersini savunmaları istenebilecek bir etkinlik düzenlemek faydalıdır. Bu, onları meydan okuma veya kişisel çatışma bileşeni olmadan kendi izlenimlerini sorgulamaya ve değerlendirilen bilginin daha derinlerine inmeye zorlayacaktır.

Önyargıların ve Duyguların Etkilerinden Kaçınmak İçin Bilgi

Dezenformasyonla mücadele, önyargılar ve duygular tarafından bilinçsizce bize dayatılan sınırlamalara karşı bilinçli ve sürekli bir mücadeledir. Bu anlamda, dezenformasyonla mücadele, kendimizi daha iyi tanımak, önyargılarımızı belirlemek ve anlamak ve bunların değerlendirme yaparken nasıl devreye girebileceğini ve bunlarla karşılaştığımızda nasıl hissettiğimizi kavramakla başlar. İstem dışı ve bilinçsiz süreçlerin farkına vardığımızda, giderek daha fazla gizlenmiş ve ayrıntılı dezenformasyonla dolu bir toplumla karşı karşıya kalırken, bunların etkisini sınırlamak için adımlar atabiliriz. Bunu yaparken, aşağıdaki tavsiyeler yardımcı olabilir:

1. Kendi önyargılarımızla mücadele edin.
2. Bir bilgiyi sadece çok kez tekrarlandığı için dikkate almaktan kaçının.
3. Bilgiyi, aile veya arkadaşlar gibi yakın çevremizden gelse bile sorgulayın.
4. Görseller varsa dikkatli olun, çünkü dikkatimizi çekerler ve değiştirilebilirler.
5. Duygularımızı tetikleyen şeylerden, özellikle öfke, korku, merak, şefkat, hayranlık veya aciliyet duygularından uzak durun, onları karantinaya alın.

Doğrulama önyargısıyla mücadele, düşüncelerimize en yakın olan daha zorlu bilgileri sorgulayarak yapılabilir, çünkü zeki varlıklar olsak da, fikirlerimizi değiştirmemeye önceden programlanmışızdır. Bu nedenle, özellikle düşünce tarzımıza uyan veya inanılması güç olan her şeyi sorgulamalıyız.

STRATEJİLERİNİZİ BİLMEK: AMACI NEDİR VE YANLIŞ BİLGİ NASIL ÇALIŞIR?

Rakibinizi tanımak, mücadelede her zaman bir avantajdır. Bu düşünce doğrultusunda, yanlış bilgi, önyargılar ve duygularla ilgili sınırlamalardan yararlanan stratejileri bilerek ve harekete geçirerek insanların rasyonel isteksizliğinin üstesinden gelme eğilimindedir. Bunun farkında olmak başlı başına olumlu bir şeydir. Bu sürecin nasıl yapıldığını belirlemeye çalışarak daha da ileriye gidilebilir.

Öte yandan, yanlış bilginin yaratılmasının ardındaki motivasyonu bilmek faydalıdır.

Bazen yanlış bilgi sadece eğlence için, bir meydan okuma olarak veya eğlence amacıyla kaos yaratmak için yaratılmıştır. Bazen de dezenformasyonun finansal veya ideolojik amaçları vardır.

Olası bir organize tehdit perspektifinden bakıldığında apaçık görünen şeyleri analiz etme yeteneğine sahip olmak gerekir. Dezenformasyonun genel amaçlarını bilmek, arkasındaki motivasyonları ve nihai etkilerini, ayrıca kullanılan olağan stratejileri analiz etmek, muhtemelen sahtekarlığı ortaya çıkarmaya ve sorumlunun hedefine ulaşmasını zorlaştırmaya yardımcı olacaktır.

Bilgileri Çapraz Kontrol Etmek İçin Araçları Bilmek ve Kullanmak

Belirli bilgilerin doğrulama sürecinin sonunda, her zaman çapraz kontrol edilmesi gereken somut veriler (meta veriler, metinsel bilgiler, resimler, ses veya video) vardır. Bu görev, aşağıdaki yeteneklerden biri veya birkaçı tarafından desteklenmelidir:

- Farklı web platformlarında veya sosyal ağlarda bilgi için verimli arama kullanımı.
- Güvenilir ve ilgili bilgi kaynaklarına erişim.
- Görüntü ve videoların hızlı çapraz kontrolü için uygulamaları ve hizmetleri bilmek ve kullanmak.
- Bilgilerin detaylı bir şekilde incelenmesi, mantıksal düşünme ve çıkarım yeteneğinin de göz ardı edilmemesi gerekmektedir.

Duruma bağlı olarak, tamamlayıcı veya alternatif prosedürler devreye sokulacaktır. Dezenformasyonu tespit etmek, bilgi sistemlerine (veritabanları veya web sayfaları) erişebilmeyi ve bir şeyin zaten sahtekarlık olarak tanımlanıp tanımlanmadığını kontrol etmeyi mümkün kılar.

DEZENFORMASYONLA MÜCADELE İÇİN ON KURAL

Temel kural şudur: Bir şeyin doğru olduğundan emin değilseniz, onu paylaşmamalısınız. Bu nedenle, bilgiyi paylaşmadan önce doğruluğunu teyit etmelisiniz. Bunu yapmak için aşağıdaki hususlar dikkate alınmalıdır:

1. Bilginin kaynağını çapraz kontrol edin. Bilmiyorsanız veya tanımlanmamışsa, dikkatli olun ve güvendiğiniz kaynaklarla çapraz kontrol edin.
2. Görünümünü değerlendirin: değiştirilmiş URL, yazım, kalite, garip veya dikkat çekici tasarımlar, tarihler vb. Taklitlere dikkat edin.
3. Bilgi güvendiğiniz birinden, aileden veya akrabalarından geliyorsa dikkatli olun. Bu bir kalite işareti değildir, çünkü çapraz kontrol edildiğinin garantisi yoktur.

İçerik

4. Sadece başlığı değil, tüm bilgileri değerlendirin. Bağlamından koparılmış alıntılara veya görsellere dikkat edin.
5. Görsellere veya videolara dikkat edin. Bunlar kolayca yanlış sunulabilir veya ilişkilendirildikleri olay veya zamanla örtüşmeyebilir.
6. Bilgileri diğer güvenilir medya veya kaynaklarla karşılaştırın. Bulamıyorsanız şüphelenin. Sağlıkla ilgili konular, uyarılar veya acil durumlar için yalnızca resmi kaynakları kullanın.
7. Kendini tamamen gerçekmiş gibi göstermek için yanlış ve doğrulanmış veya doğrulanabilir verileri karıştıran bilgilere dikkat edin.

Kasıt

8. Öfke, endişe veya aciliyet duygularını tetikleyen bilgilere karşı dikkatli olun. Bu, dezenformasyon üretenlerin sıklıkla başvurduğu bir stratejidir.
9. Çok iyi veya çok şaşırtıcı haberler ve bilgiler de dezenformasyonu gizlemenin bir yoludur. Analizinizde objektif kalın.
10. Mizah ve hicvi belirleyin. Bu tür haberleri şaka şeklinde sunan ve bunu profesyonelce yapan, ancak her zaman tarafsız olmayan web sayfaları var.

DiJiTAL AYAK izi



Dijital Ayak İzi, İtibar ve Dijital Kimlik

Hayatımızı giderek daha fazla dijital ortamda yaşıyoruz. Bazen bu, çevrimdışı yaşamımızın bir devamı veya ayrılmaz bir parçasıdır. Ancak diğer durumlarda, hayatımızın iki tarafının da pek ortak noktası yok gibi görünüyor. Ya ortam bu sürekliliğe izin vermediği için ya da internet, tüm olanakları, kuralları ve içinde yaşayan insanlarıyla, davranışlarımızı, hayatımızı ekranın her iki tarafında da farklı kılıyor veya farklı gösteriyor. Her durumda, her iki senaryoda da devam eden tek şey bizim hayatımızdır. Bu nedenle ve görünürdeki bağımsızlığına rağmen, bir tarafta yapılanlar genellikle diğer tarafta dayankı bulur, yansır.

İnternette, yaptıklarımızın dijital bir izini bırakıyoruz. Belirli ortama veya sosyalleşme grubuna bağlı olarak hayatımızın farklı yönlerini gösterebiliyoruz. Başkaları, biz farkında olmadan hakkımızda bir fikir oluşturuyor. Dijital kişiliğimiz, birinin geleceğini belirleyebilecek çok önemli bir şeydir. Dijital bilgi zaman içinde kalıcıdır, sınırsız erişime sahiptir ve en yüksek hızda yayılır. Ancak birçok insan, özellikle de gençler, internette bıraktıkları hayat izlerinin önemini düşünmezler. Bu durum, kısa, orta ve uzun vadede onlara rahatsızlık verebilir.

UNUTMAYIN

- Çok genç insanlar, eylemlerinin orta ve uzun vadeli sonuçlarını düşünmek için gerekli yaşam deneyimine sahip değildirler. Çevrimiçi yaşamlarını belirli bir potansiyel kitle (tanıdık veya tanımadık) için belirli bir an için hisseder, yaşar ve paylaşırlar.
- Çocuklar ve ergenler, bıraktıkları izlerin veya yansıttıkları imajın gerçek bir bağlamda veya onları tanıma fırsatı bulamamış insanlar üzerindeki sonuçlarını görselleştirme kapasitesine sahip değildirler. Bu konuda onlara yardımcı olmalıyız.
- Teknolojinin sağlıklı kullanımına yönelik eğitim verilmesi gereklidir. Bu eğitim, eleştirel tutumların geliştirilmesine olanak tanır.
- Sosyal baskılar (moda ve alışkanlıklar) ve ticari çıkarlar, hayatlarımızı sürekli, aşırı ve hatta kompulsif bir şekilde çevrimiçi olarak paylaşmaya teşvik eder.
- Gizlilik ve siber güvenlik de, her bireyin dijital kimliğinin, itibarının ve dijital izinin bir parçası olup olmayacağının, gönüllü veya gönülsüz olarak belirlenmesinde önemli faktörlerdir.

- Dijital iz, itibar ve dijital kimlik, bir kişinin yayınladıklarının ötesine geçen çeşitli unsurları içerir. Nerede etkileşimde bulundukları, kimlerle etkileşimde bulundukları, yaptıkları yorumlar veya hatta yaptıkları veya yapmadıkları şeyler bile ilgili veriler olabilir.

TANIM VE ÖZELLİKLER

Dijital Ayak İzi

Web sayfalarını ziyaret etmek, Google gibi hizmetleri kullanmak, cep telefonunuza belirli bir uygulama yüklemek, resim yüklemek, konumumuzu kontrol etmek, görüntülü arama yapmak, "Beğen"e tıklamak veya bir blogda bir gönderi okumak, İnternet ile etkileşim kuran hizmetler, programlar ve dijital platformlar sayesinde mümkün olmaktadır. Bunların hepsi bir iz bırakır. Eylemler veya süreçler anlık ve "benzersiz" olsa da, bıraktıkları iz, yani dijital ayak izi sonsuza dek saklanabilir. Sadece çevrimiçi olmakla bile sayısız iz bırakıyoruz. Bu izler çeşitli aktörler tarafından farklı şekillerde saklanır ve bunlara herkese açık veya özel olarak erişilebilir. Ancak, her "adım", zaman içinde aynı türden veya o anki farklı türden diğerleriyle birleştirilebilir, böylece her seferinde daha önemli ve ilgili bilgiler sağlayabilirler. Tıpkı çeşitli yolların rota tercihlerimizi açığa çıkarabilmesi gibi, bir dizi ayak izi de bir yolu ve hatta o yolda nasıl ilerlendiğini tarif eder. Farklı gerçekliklere işaret eden ve farklı kaynaklardan gelseler bile aynı kişiye atfedilebilen verilerin birleştirilmesi, yüksek katma değerli ek bilgiler ortaya çıkarabilir.

Kısacası, internetteki varlığımız özel kuruluşların ve şirketlerin anonim veya kimlik bilgileriyle ilişkilendirilmiş şekilde kaydedebileceği bir iz bırakır. Çoğu durumda, bu işlemin yapılması için onayımız gerekir ve biz bu onayı neredeyse farkında olmadan veririz. Söz konusu iz, çeşitli amaçlarla saklanır. Bu saklama işlemlerinin temel nedenleri arasında maddi kazanç elde etmek, internet kullanımını belirli koşullara bağlamak ve sunulan hizmetin ya da deneyimin kalitesini ve verimliliğini artırmak öne çıkar. Bu nedenle dijital ayak izimiz hem çevrimiçi hem de çevrimdışı dünyada karşımıza çıkabilecek fırsatları etkileyerek, bugünümüzü ve geleceğimizi olumlu ya da olumsuz yönde şekillendirebilir.

Dijital Kimlik

Bir kişinin dijital kimliği, en basit tanımıyla internetin bize bu kişi hakkında anlattığı şeydir. Başka bir deyişle, internette bu kişiye erişirken veya onu ararken bu kişiye atanabilecek veri ve özellikler kümesidir.

Bu kimlik, bir kişiyi tanımaya ayırdığınız zamana ve onun hakkında edinebileceğiniz bilgilere bağlı olarak, daha kapsamlı veya daha az kapsamlı veya ayrıntılı olabilir. Bazen bir kişi hakkındaki bilgi kapsamlı olabilir, ancak o kadar kısmi olabilir ki, yalnızca önyargılı veya hayatının belirli bir bölümüne erişebiliriz.

Bir kişi hakkında bilginin en sık bulunduğu internetteki iki yer şunlardır:

- (Google gibi) tarayıcılar, bilgiyi doğrudan içermez, ancak onu bulmaya yardımcı olur. Bu amaçla, süreci optimize etmek için bu bilgilerin bazı bölümlerinin küçük geçici kopyaları oluşturulur. Arama motorları, web sayfalarında ve bunu yapmalarına izin veren diğer hizmet ve platformlarda bulunan bilgileri kataloglar ve indeksler.
- Sosyal ağlar ve platformlar, genel olarak bilgilerin somut bir profille ilişkilendirildiği ve kişilerin etiketler veya takma adları veya kullanıcı adları kullanılarak tanımlanmasının yaygın olduğu büyük veri tabanlarından başka bir şey değildir.

Bu nedenle, bir kişinin dijital kimliğini görmenin en basit yolu, tarayıcılar ve sosyal platformlar tarafından döndürülen bilgi kümesidir. Dijital kimlik, kişinin başkalarıyla ilişkilerini ve dolayısıyla hayatının ilgili yönlerini etkileyebilir. Bu anlamda dijital kimliğimizi geliştirmek ve ona özen göstermek önemlidir.

Dijital Kimliği Oluşturan Unsurlar

Dijital kimliğin, bir kişi hakkında yayınlanan, kendisi veya başkaları tarafından tanımlanabilen verilerin (çoğunlukla metin, resim veya video) ötesine geçtiğini hatırlamak önemlidir. Bu en açık ve tanınabilir kimliği oluşturur. En eksiksiz dijital kimlik, aşağıdakiler gibi diğer unsurlarla da belirlenir:

- Kullanıcı adı, profil resmi ve durumunun tanımlandığı, tanıtıldığı veya duyurulduğu kısa metin.
- Etkileşimde bulunduğu kişiler.
- Bir kişinin profilinin bulunduğu veya katılım sağladığı yerler ya da platformların yanı sıra; yaygın olmalarına rağmen kaçınılan veya kullanılmayanlar.
- Kişinin kimliğinin belirlenebileceği kapalı veya açık platformlarda yapılabilecek yorumlar ve etkileşimler (beğenme, gönderme vb.).
- Açıkça erişilebilir olabilecek herhangi bir dijital ayak izi.

Dijital Kimliğin Özellikleri

Bir kimliği oluşturan unsurların doğasına ek olarak, nasıl davrandığını ve nasıl etkileyebileceğimizi bilmek için hangi özelliklere sahip olduğunu bilmek önemlidir:

- Farklı Versiyonlarla

Dijital kimlik, yukarıda belirtildiği üzere, analiz edilen verilerin miktarına, türüne ve niteliğine bağlı olarak az ya da çok ayrıntılı veya kapsamlı olabilir. Ayrıca, sınırlı ve somut bilgi kaynaklarına dayanıp dayanmadığına bağlı olarak daha bütüncül ya da yalnızca kısmi bir nitelik taşıyabilir.

- Dinamiklik

Dijital kimlik dinamiktir ve zamanla değişir. Onu oluşturan bileşenler değiştirilerek dijital kimlikte değişiklik yapmak mümkündür ancak genellikle, dijital kimliğe yeni nitelikler veya bilgiler eklemek, mevcut olanları çıkarmaktan daha kolaydır. Dijital kimlik içeriğini oluşturan bilgilere erişim biçimini etkileyen teknik koşullar, platformların kullanımı veya bizzat platformların indeksleme yöntemlerindeki değişiklikler gibi, internet kullanıcılarıyla doğrudan ilişkili olmayan unsurlardan etkilendiğinde de değişime uğrar. Buna somut bir örnek olarak, belirli bir sosyal ağın herhangi bir zamanda kendi içeriğinin ve veritabanlarının indekslenmesine izin verme veya bunu engelleme kararı alması gösterilebilir.

- Artan karmaşıklık

Sosyal ağların yaygınlaşması, bireylerin daha karmaşık bir dijital kimliğe sahip olmalarını da beraberinde getirdi. İnsanlar artık daha belirgin, basit ve düzenli bir şekilde paylaşımlarda bulunup başkalarıyla etkileşime girdikleri için, dijital kimlikler de daha fazla unsurdan oluşmaktadır.

- Güçlülükle kontrol edilebilen bir yönetim süreci

Sosyal ağların mümkün kıldığı etkileşimler, dijital kimliğin bizzat sahibi veya ilgili kişi tarafından kontrol edilmesini zorlaştırmış ve bu kimliği, başkalarının onunla ilgili eylemlerine daha bağımlı hale getirmiştir. Zira bu sosyal platformlardaki tüm etkileşimler belirli profillerle ilişkilendirilmekte olup somut ve tanımlanabilir niteliktedir. Buna örnek olarak, bir kişinin sosyal ağda başka bir bireyi etiketlemesi durumunda, bu eylem söz konusu kişinin mahremiyetini olumlu ya da olumsuz etkileyebilse de onun dijital kimliğine bir şekilde katkıda bulunduğunu söyleyebiliriz.

Dijital İtibar

Dijital itibar kavramı, bir kişinin dijital yaşam serüvenine dayalı olarak başkaları tarafından algılanma biçimiyle ilişkilidir. Bu kavram, bir kişi hakkında çevrimiçi ortamda açığa çıkan bilgileri kapsamı bakımından dijital kimlikle bağlantılıdır, ancak daha geniş bir zaman boyutunu ve az ya da çok öznel bir değerlendirmeyi de içerdiği için bunun ötesine geçer. İtibar, verilerin yalnızca belirli bir andaki konumu veya algılanışına değil, zaman içindeki değerlendirmesine işaret eder.

Dijital itibarın önemi, çevrimiçi ve çevrimdışı ilişkilerimiz ile fırsatlarımız söz konusu olduğunda dijital kimliğin önüne geçebilmesinde yatar. Başka bir deyişle, bir kişinin şu anda veya belirli bir bağlamda nasıl görüldüğünden ziyade, internetin o kişinin geçmişte nasıl biri olduğuna dair "söyledikleri" daha önemli olabilir. Bu durum çevrimdışı dünyada da geçerli olabilir. Ancak yine de ortada, internetin bir kişinin az ya da çok uzak geçmişine ait belirli verileri veya olayları kaydetme, saklama ve daha da önemlisi bunları yeniden ön plana çıkarma konusundaki benzersiz kapasitesi gerçeği durmaktadır.

İnternette geçirdiğimiz sürenin, gelecekteki yaşamımızı etkileme potansiyeline sahip, neredeyse silinmez bir iz bıraktığının bilincinde olmak, erken yaşlardan itibaren büyük önem taşımaktadır. Özellikle de hız ve aniliğin, orta ve uzun vadeli sonuçlar üzerine derinlemesine düşünmeyi ve öngöründe bulunmayı engellediği bir dünyada.

BUNU ÖNLEMEK VE DURUMA MÜDAHALE ETMEK İÇİN NELER YAPILABİLİR?

İşin içindeki Unsurların Ve Bunlar Arasındaki İlişkilerin Farkına Varmak

Pek çok kişi özellikle de çocuklar ve ergenler iyi niyetle hareket ettiklerini ve saklayacak hiçbir şeyleri olmadığını ifade eder. Buna bağlı olarak dijital ayak izleri, itibarları veya dijital kimlikleri konusunda endişelenmelerine gerek olmadığını savunurlar.

Bu bağlamda, üç temel hususun vurgulanması gerekir:

- Mahremiyet, kişiyi koruyan bir unsurdur. Bir kişi hakkında ne kadar çok şey bilinirse, o kişi o kadar savunmasız hale gelir.
- Siber güvenlik, mahremiyeti güvence altına almak için gereklidir aynı zamanda mahremiyet de siber güvenliğin bir güvencesidir.
- Mahremiyet ve siber güvenlik, grup ilişkilerini düzenleyen kolektif meselelerdir. Başkalarının bu konulardaki eylemleri bizi etkileyebilir ve aynı şekilde bizim eylemlerimiz de onları etkileyebilir.

Bu doğrultuda, her bireyin dijital ayak izi, kimliği ve dijital itibarı; internette kendilerine dair iz bırakan bilgiler ve eylemlerle şekillenir. Söz konusu iz ise hem bireyin kendisine hem etkileşimde bulunduğu kişilere hem de kullandığı platform veya hizmetlere bağlıdır.

DİJİTAL İZLE HANGİ SORUNLAR İLİŞKİLENDİRİLEBİLİR?

Bir kişinin dijital izi, bu izin bir kısmına sahip olan herhangi bir tarafça kullanılabilir. Dijital iz ilgili kişiye sunulan hizmet veya bilgi türlerine ve kişinin bunları hangi yöntemlerle ve hangi koşullar altında kabul ettiğine dair bir profil oluşturur. Bu durum bir avantaj ya da ciddi bir dezavantaj teşkil edebilir. "Bilgi güçtür" ilkesi göz önünde bulundurulduğunda dijital iz şeklinde geride bıraktığımız bilgilerin bir kısmının kötü niyetli bir şirket veya şahsın eline geçmesi, bu bilgilerin kötüye kullanılmasına yol açabilir. Aynı zamanda söz konusu tarafa, ilgili kişi ya da siber suç mağduru adayı üzerinde büyük bir güç ve avantaj sağlamasına yol açabilir. Ayrıca, çoğu zaman geride bıraktığımız izlerin farkında olmadığımız, bunlardan haberdar olma, bunları değiştirme veya silme imkânına sahip bulunmadığımız da hesaba katıldığında, dijital izlerin son derece önemli bir varlık ya da potansiyel bir güvenlik açığı olduğu söylenebilir.

DİJİTAL AYAK İZİNİ NASIL AZALTABİLİRİZ?

Geride bıraktığımız ayak izini belirlemek veya bunu kendi lehimize çevirmek kolay değildir. Bu nedenle, dijital ayak izimizden olumsuz etkilenmekten kaçınmanın tek yolu onu azaltmaktır. Bunu yapmanın üç yolu vardır:

- İz bırakma durumlarını azaltmak. Bu, internete bağlı dijital cihazların ve hizmetlerin kullanımını azaltmak anlamına gelir. Bu her zaman mümkün olmayabilir, ancak bunu yapmanın açık fırsatları vardır.
- Akıllı hoparlörler veya belirli bir uygulama gibi çok fazla değer katmayan akıllı ve otomatik dijital hizmetleri kullanmamak.
- Hizmetleri, cihazları ve uygulamaları en kısıtlayıcı şekilde ayarlayarak veri yakalamayı kısıtlamak. Bu, birçok durumda ne kolay ne de kullanışlıdır. Örneğin, coğrafi konum belirlemeyi devre dışı bırakmak bir yöntem olabilir.

Olumsuz Bir İtibar ve Dijital İz İle İlişkili Sorunlar Neler Olabilir?

Dijital kimliğimizin ve itibarımızın karşılaştığı zorluklar; bir kişinin gerektiği her yerde doğru ve olumlu bir şekilde tanımlanabilmesi ve başkalarının o kişi hakkındaki algısının olumlu olması gerekliliğiyle ilgilidir. Durumun böyle olmaması halinde, yanlış yerde veya zamanda hatalı bir şekilde tanımlandıkları için bireyin fırsatları azalır. Hatta sırf itibarları nedeniyle elenmeleri bile söz konusu olabilir.

İyi Bir Dijital Kimlik ve İtibar Nasıl Oluşturulur?

Dijital bir kimliğe sahip olmak ve olumlu bir itibarı korumak kolay bir iş değildir. Bu süreç, bazen akıntıya karşı kürek çekmeyi gerektiren sürekli bir çaba ister ve diğer

insanlar da dahil olmak üzere çeşitli faktörlere bağlıdır. Yine de bu konuda yardımcı olabilecek on dört öneri sıralanabilir. Bunlar aşağıda listelenmiş ve üç kategori altında gruplandırılmıştır:

Temel Bilgiler

1. Çevrimiçi ortamda kendinizi sunma şeklinize özellikle dikkat edin. Profil fotoğrafınız, takma adınız ve giriş cümleiniz veya durumunuz her zaman saygılı ve olumlu olmalıdır.
2. Cihazlarınızdaki, uygulamalarınızdaki ve sosyal ağlarınızdaki gizlilik ve siber güvenlik şartlarına dikkat edin. Şartlar ne kadar katıysa, kontrol o kadar fazladır.
3. Özellikle öfke veya aşırı coşku gibi duygulara kapıldığınızda, bir şey yayınlamadan önce iki kez düşünün.
4. Bir şey yayınlamadan önce, bunun şimdi veya gelecekte kamuoyuna açık olarak görülmesi durumunda ne gibi bir etki yaratabileceğini düşünün, tahmin edin ve hayaledin.
5. Dijital vatandaşlığınızı doğru, bağlamlı ve bilgili bir şekilde kullanarak aktif olarak katılın, çünkü bu bir iz bırakacaktır.
6. Dijital bir izi silmenin kolay olmadığını unutmayın, çünkü başkaları tarafından yakalanıp yeniden üretilebilir veya basitçe, silme işlemi sizin elinizde olmayabilir.

Başkalarıyla ilgili olarak:

1. Başkalarının gizliliğinize saygı duyması konusunda ısrarcı olun. Bu, dijital itibarınızı ve kimliğinizi minimum düzeyde yönetebilmenin en iyi garantisidir.
2. Ne yaptığınızı yayınlama baskısı veya ihtiyacı hissetmekten kaçının. Hayatınız hakkında çevrimiçi olarak ne paylaştığınızı, ne kadar, nasıl ve kiminle paylaştığınızı akıllıca yönetin.
3. Etkileşimde bulunduğunuz kişilerin ve platformların gizliliklerini ve siber güvenliklerini nasıl yönettiklerinin sizi de etkilediğini unutmayın.
4. Özellikle başkalarını etkileyen, özellikle de tanınabilir kişileri etkileyen şeyler yayınlarken çok dikkatli olun.

Proaktif bir şekilde olumlu olun:

1. Olumlu bir dijital kimlik ve itibar geliştirin. Gelecekte bakmaktan gurur duyacağınız her şeyde görünür bir iz bırakın.
2. Kendinizi düzenli olarak internette (tarayıcılar, çeşitli sosyal ağlar ve platformlar vb.) arayın ve kendiniz hakkında neler bulunabileceğini kontrol edin.
3. Sizin gibi kişilerin katıldığı platformlarda profil oluşturun. Kimliğinizi korumak ve taklit edilmekten kaçınmak için olumlu olabilir.

4. Belirli veya geçici şeyler için farklı profiller ve kimlikler yönetin. Bu olumlu olabilir.

OLUMLU BİR DİJİTAL İTİBAR VEYA KİMLİK İÇİN ON ÖNERİ

Sürekli olarak dijital bir kimlik veya itibar geliştirmek oldukça zor olabilir. Özellikle de, değerleri ve alaka düzeyleri geliştirme aşamasında kolayca algılanamıyorsa. Bu nedenle, net bir şekilde belirlenmiş bir kimliğe sahip olmak önemlidir.

1. Seçici olun ve yayınladıklarınızı azaltın.
2. Uygun ayarları ve kanalları seçerek yayınlarınızın kapsamını yalnızca gerekli kişilerle sınırlandırın.
3. Bir şey yayınlamadan önce hayali bir küresel kitleyi (herhangi birini) ve zamansız bir etkiyi (her zaman) göz önünde bulundurun.
4. Herhangi bir uygulamayı indirmeden önce, verilerinizi nasıl işlediklerini öğrenin.
5. Kendi gizliliğinize ve siber güvenliğinize, ayrıca etkileşimde bulunduğunuz diğer kişilerin gizliliğine ve siber güvenliğine dikkat edin ve özen gösterin.
6. Olumlu bir tutum ve üslup sergileyin. Bu daha sağlıklıdır ve sizi daha saygın kılar.
7. Yoğun veya olumsuz duygulara kapıldığınızda bir şeyler yayınlamaktan kaçının.
8. Gereksiz çatışmalardan kaçının.
9. Farklı ortamlar ve amaçlar için farklı profiller oluşturun.
10. Nasıl görüldüğünüzü öğrenmek için sosyal platformlarda kendinizi arayın.

Kaynakça: UNODC. Birleşmiş Milletler Uyuşturucu ve Suç Ofisi. Kasım 2022



www.imef.org.tr
info@imef.org.tr