UNFPA

UN WOMEN

TÜM KADINLAR VE KIZ ÇOCUKLARI İÇİN

Dijital Şiddet/ Teknoloji Destekli Cinsiyete Dayalı Şiddet Rehberi



Bu rehber kimin için?

Senin ve herkes için...

Bu rehberle sana, dijital şiddet hakkında bilgi vermek ve dijital alanlarda kontrolü ele alman için yol göstermek istiyoruz.

DİJİTAL ŞİDDETE NOKTAYI KOY!

Yazarlar: Nurcihan Temur, Pınar İlkiz
Genişletilmiş ve Güncellenmiş Baskı – 2025
İlk Yayın: Toplumsal Cinsiyete Dayalı Siber Şiddet Rehberi (UN Women, 2020)

Bu rehber, UN Women Türkiye ve UNFPA Türkiye tarafından yürütülen 'Kadınlara ve Kız Çocuklarına Yönelik Dijital Şiddete Noktayı Koy' kampanyası kapsamında hazırlanmıştır. Rehber, Norveç ve Yeni Zelanda Hükümeti'nin finansal desteğiyle, dijital şiddet konusunda kavramsal bütünlük sağlamak amacıyla düzenlenen "Dijital Çağda Şiddeti Yeniden Düşünmek" adlı atölyenin çıktılarına dayanmaktadır.

Bu yayının tüm hakları Birleşmiş Milletler Kadın Birimi (UN Women) ve Birleşmiş Milletler Nüfus Fonu'na (UNFPA) aittir. Bu çalışma, UN Women ve UNFPA'in yazılı izni alınmadan, kısmen veya tamamen kopyalanamaz, çoğaltılamaz veya yayımlanamaz. İlgili kaynağa atıf yapılması koşuluyla yayından alıntı yapılabilir. Bu yayında yer alan içeriklerin sorumluluğu yazarlara ait olup, UN Women, UNFPA, Birleşmiş Milletler ve bağlı kuruluşların resmi görüşlerini yansıtmak durumunda değildir.

---

5 – 6 Kasım 2025 tarihlerinde düzenlenen sivil toplum kuruluşlarına ve genç aktivistlere destekleri ve katkıları için teşekkür ederiz: Alternatif Bilişim Derneği, Aramızda Toplumsal Cinsiyet Araştırmaları Derneği, Damla Göksu, Başkent Gençlik Meclisi, Beyza Doğuç, Cinsel Şiddetle Mücadele Derneği, Havle Kadın Derneği, Hayat Sende Derneği, İstanbul Barosu, İstanbul Toplumsal Cinsiyet Müzesi, Kaos GL, Kadın Dayanışma Vakfı, KızBaşına, UNFPA Mülteci Destek Hizmet Birimi, SGDD-ASAM, SistersLab - Bilim ve Teknolojide Kadın Derneği, SPoD, Ted Universitesi Toplumsal Cinsiyet Çalışmaları Merkezi, Türkiye Kadın Dernekleri Federasyonu, Uçan Süpürge Vakfı, ÜniKuir, Zincir Sosyal Girişim, UN Volunteers – Birleşmiş Milletler Gönüllüleri: Ada Derya Üstün, Aslı Akbay Alagöz, Elifnur Çağlayan, Elif Sinem Özel

Önce tanımlardan başlayalım mı?

Kadınlara yönelik şiddet, Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşmesi (CEDAW) başta olmak üzere birçok uluslararası ve ulusal sözleşme tarafından kadınlara karşı ayrımcılık ve bir insan hakları ihlali olarak tanımlanıyor. Kadınların, kadın olmalarından dolayı maruz bırakıldıkları bir şiddet türü olan kadınlara yönelik şiddet, kadınları orantısız bir biçimde etkiliyor.[1]

"Dijital şiddet" ya da daha geniş tanımı ile "teknoloji destekli cinsiyete dayalı şiddet", bilgi iletişim teknolojileri veya diğer dijital araçların kullanımıyla işlenen, desteklenen, ağırlaştırılan veya güçlendirilen, sonucunda fiziksel, cinsel, psikolojik, sosyal, politik veya ekonomik zarar doğuran veya doğurması muhtemel olan veya hak ve özgürlüklerin başka ihlallerine yol açan her türlü eylem olarak tanımlanmaktadır.[2]

Bu rehberde Türkiye'de yaygın kullanılan "dijital şiddet" ifadesi ile Birleşmiş Milletler'in "teknoloji destekli cinsiyete dayalı şiddet" tanımı birlikte kullanılmaktadır. Kavram için uluslararası ölçekte tek bir tanım bulunmadığından, literatürde "siber şiddet", "dijital şiddet" ve "teknoloji destekli kadına yönelik şiddet" gibi farklı terimlere de rastlanmaktadır.

- Dijital şiddet, gerçektir!
- Olayların dijital ortamlarda yaşanması şiddetin derecesini azaltmaz!
- Toplumsal cinsiyete dayalı şiddetin her türlüsü gibi dijital şiddet de bir insan hakları ihlalidir ve eşitsizliklerin bir sonucudur!
- Dijital şiddet, dijital uçurumu derinleştirerek bilgiye ve hizmetlere erişimi kısıtlar, kadınların kamusal yaşama eşit biçimde katılma hakkını ihlal eder!

Dijital şiddeti diğer şiddet biçimlerinden ayıran özellikler nelerdir?

Dijital şiddet, diğer cinsiyete dayalı şiddet biçimleriyle ortak özellikler taşısa da (cinsiyete dayalı olması, yaygın olması gibi) dijitalin doğasıyla ilgili belirgin özelliklere sahiptir:[3]

- **Anonim** olabilir,
- **Uzaktan** uygulanabilir (fiziksel temas olmadan dünyanın her yerinden işlenebilir),
- Failler için **kolay erişilebilir** (failler için maliyeti ve zorluğu düşüktür),
- Yayılma **hızı yüksektir** (internet üzerinden kolayca yayılır, şiddete maruz kalanları yeniden travmatize eder),
- **Cezasızlık riski** barındırır,
- **Otomasyona** açıktır (sınırlı zaman ve çabayla otomatikleştirilebilir),
- **Kolektif** olarak organize edilebilir,
- Şiddetin **normalleşmesine** katkı sağlar (şiddetin dijital alanda daha az ciddi algılanmasına katkıda bulunur),
- **Sürekli** olabilir (görüntüler ve dijital materyaller süresiz olarak varlığını sürdürebilir).

Dijital dünyadaki yeni riskler nelerdir?

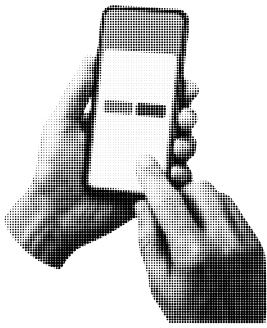
Hızlı teknolojik değişimler, dijital şiddeti arttıran yeni risk ve platformları karşımıza çıkarmaktadır[4]:



Kadın Hakları Karşıtı Grupların Yükselişi

Kadın haklarına karşı çıkan bazı aktörler, çevrim içi alanları giderek daha fazla kullanmaktadır. Bu durum, kadınlar ve kız çocukları için taciz ve şiddet tehditleriyle belirginleşen düşmanca bir dijital ortam yaratmaktadır. Kadın siyasetçiler, kadın hakları aktivistleri, kadın gazeteciler ve kamusal alanda görünür olan kadınlar bu saldırıların doğrudan hedefi haline gelmektedir.

Yapay Zekanın (AI) Etkisi



Yapay zekanın hızlı gelişimi, yanlış bilgi ve hedefli dezenformasyonun yayılmasını kolaylaştırmaktadır. Bunun yanında, yapay zeka ile üretilen sahte görüntüler (deepfake) ve rızaya dayalı olmayan içerikler de giderek artmaktadır.
Sensity AI verilerine göre, çevrim içi sahte videoların **%90-95**'i rızaya dayalı olamayan cinsel görüntülerden oluşuyor ve bunların yaklaşık **%90**'ı kadınları hedef alıyor.[5]



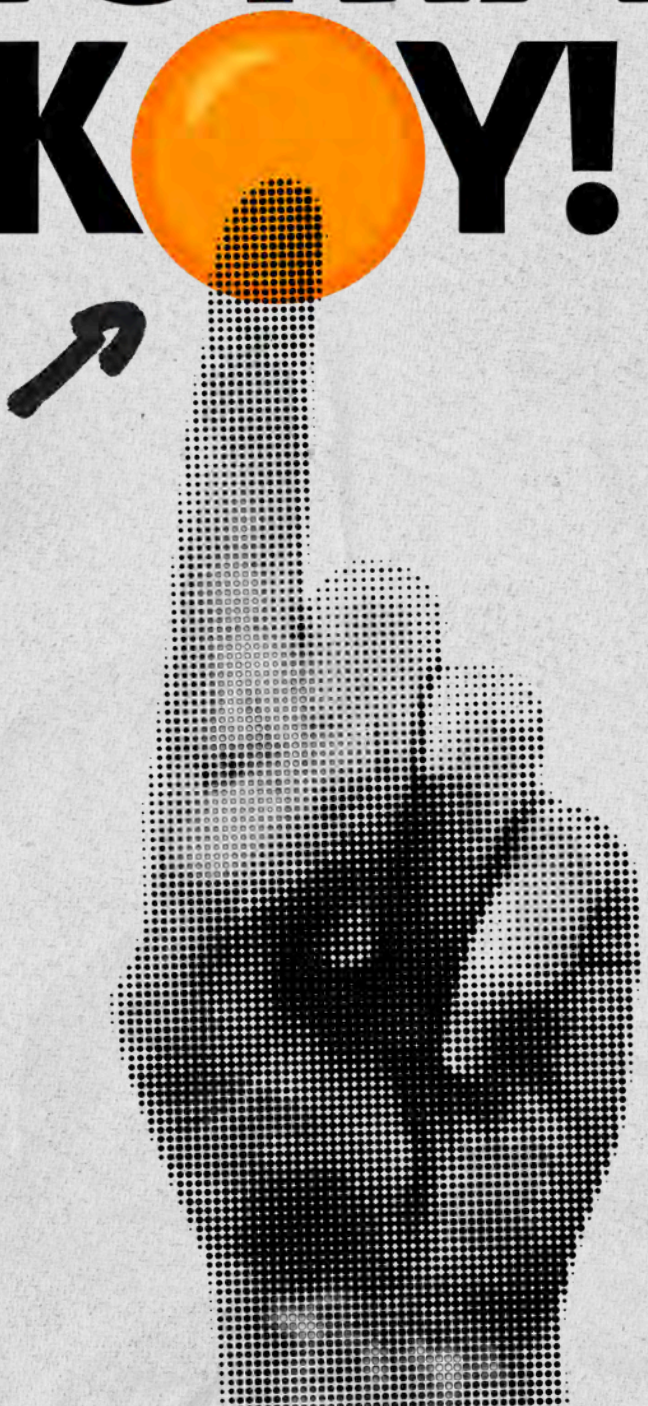
Mizojonist Tutumlarda Artış

Teknoloji, kadın düşmanı (mizojinist) toplumsal normları güçlendirmekte bir araç olarak kullanılmaktadır. Son çalışmalar, çevrim içi alanların kadın düşmanlığını beslediğini ve kadınlara yönelik şiddetin normalleşmesini pekiştirdiğini göstermektedir.
Örneğin "Manosphere" olarak adlandırılan çevrim içi erkek toplulukları ağı (erküre/dijital erkekçilik evreni), farklı platformlara yayılmış, merkezi olmayan bir yapıdır. Bu ağ, cinsiyetçi kalıp yargıları popüler ve kolay paylaşılabilir biçimlerde çoğaltmakta, faillerin anonimliği nedeniyle hesap verilebilirliği sınırlı hale getirmektedir.

- 31 ülkede yapılan bir araştırmada genç erkeklerin, cinsiyet eşitliğini savunmanın erkeklere karşı bir ayrımcılık oluşturduğunu düşündüğü ortaya koyuyor. [6]

- 2022'de yapılan bir başka çalışma ise şiddet içeren söylemlerde bir önceki yıla kıyasla **%59** artış ve çocukların cinsel istismarını teşvik eden içeriklerde de artış olduğunu ortaya koymuştur. [7]

DİJİTAL ŞİDDETE NOKTAYI KOY!



Dijital şiddete kim maruz kalıyor?

Herkes!
Ancak dijital şiddet, toplumsal cinsiyete dayalı şiddet ile aynı yapısal eşitsizliklerden ve ayrımcılıktan kaynaklandığı için kadınların ve kız çocuklarının maruz kaldığı şiddet daha farklı ve fazladır.

- Küresel ölçekte karşılaştırılabilir veriler sınırlı olsa da, dijital ortamda kadına yönelik şiddetin görülme oranı **%16** ile **%58** arasında değişmektedir.[8]

- UN Women'ın Kasım 2023'te yayınladığı "Dijitalleşmenin Karanlık Yüzü: Doğu Avrupa ve Orta Asya'da Kadınlara Yönelik Teknoloji Destekli Şiddet" raporuna göre araştırmaya dahil olan 12 ülkenin ortalaması teknoloji destekli şiddete maruz bırakılan kadınların oranı ortalama %53.2'dir. Türkiye'de ise bu oran %72.4'tür.[9]

- UNFPA tarafından desteklenen ve 2021'de Toplumsal Bilgi ve İletişim Derneği tarafından yayınlanan "Türkiye'de Dijital Şiddet Araştırması"nın sonuçlarına göre ise kadınların %51'i dijital ortamlarda yazılı, sesli veya görüntülü taciz mesajları alıyor, %46'sı ısrarlı takibe uğruyor.[10]

Kimler daha fazla risk altında?

Yakın partner şiddetine maruz bırakılan kadınlar en yüksek risk grubundadır ancak dijital ortamlarda bazı grupların orantısız biçimde hedef alındığı da görülmektedir. [11]

Lider kadınlar:

Dijital ortamlarda daha görünür olan kadınlar, dijital şiddete daha fazla maruz kalmaktadır.
Siyasetçi, gazeteci, sanatçı, yazar, akademisyen, sporcu ve aktivist kadınlar, dönem dönem dijital şiddet faillerinin açık hedefi haline gelebilmektedir.

- UNESCO'nun araştırmasına göre, kadın gazetecilerin **%73**'ü çevrim içi şiddete maruz kalmıştır.[12]
- Uluslararası Parlamentolar Birliği'nin verilerine göre kadın siyasetçilerin **%81.8**'i çevrim içi tacize uğramış, **%44.4**'ü cinsel-fiziksel şiddet tehdidi almıştır.[13]

Genç kadınlar ve kız çocukları:

Gençler dijital açıdan çok daha aktifler ve bu durum onların dijital şiddete maruz bırakılma risklerini artırıyor.

- 15-25 yaş arası genç kadınların ve kız çocuklarının **%58**'i çevrim içi tacize uğramıştır. **%85**'i ise birden fazla türde dijital şiddet türüne maruz kalmıştır.[15]

Kesişen kimliklere sahip kadınlar ve kız çocukları:

Kadınlar ve kız çocukları; yaş, meslek, eğitim, engellilik, ırk veya etnik köken, göçmenlik durumu, cinsiyet kimliği ve sosyal konum gibi kesişen özellikleri nedeniyle dijital şiddete farklı biçimlerde ve orantısız düzeylerde maruz kalabilmektedir.

"Özellikle sosyal medya aracılığıyla uygulanan şiddet, kadın siyasetçilerin konumları ve güçleriyle doğru orantılı olarak artmakta; bilhassa daha görünür olan kadın siyasetçilere yöneltilen söz konusu şiddet, ***diğer kadınların siyasete katılımı açısından cesaret kırıcı olabilmektedir.*** *Bu anlamda* ***bir kadın siyasetçinin maruz bırakıldığı şiddet, başka bir kadının siyasete katılımına dolaylı bir engel yaratabilmektedir."***
(Türkiye'de Siyasette Kadınlara Yönelik Şiddet - UN Women, 2023[14])

Dijital şiddeti uygulayan kim(ler)?

Dijital şiddeti uygulayan kişi, eski ya da şu anki eş / partner, komşu, iş / okul arkadaşı, bir yakın ya da bir yabancı olabilir.

Dijital şiddetin büyük bölümü, bilinmeyen kişiler (%50,3) veya yalnızca internette tanınan kişiler (%17,5) tarafından uygulanmaktadır. Ancak teknoloji destekli şiddetin neredeyse üçte biri (%32,1), partnerler, aile üyeleri, arkadaşlar, tanıdıklar, iş arkadaşları, yöneticiler veya okul arkadaşları gibi kadınların sosyal çevresindeki kişiler tarafından gerçekleştirilmektedir ve bu nedenle çevrim dışı şiddetin bir uzantısıdır.[16]

Dijital şiddet bizim hatamız değildir!

Şiddet suçtur ve şiddet uygulayanlar için çeşitli yaptırımlar vardır!

Failler, farklı taktik ve araçlar kullansalar da, amaç değişmiyor: **utandırmak, aşağılamak, korkutmak, tehdit etmek, susturmak veya linç saldırılarını ya da kötü niyetli yakınlaşmaları cesaretlendirmek.** Tüm bu eylemler, kişinin güvenliğini ve ifade özgürlüğünü hedef alan aynı güç ve kontrol mekanizmasının parçasıdır.

Dijital şiddet nerede ve nasıl gerçekleşir?

Dijital şiddet eylemleri, sosyal medya ve mesajlaşma platformları, uygulamalar, oyunların sohbet odaları, forumlar ve e-posta gibi Bilgi ve İletişim Teknolojileri'nin (BİT) kullanılmasıyla gerçekleşir.



- Failler genellikle kontrolü sürdürme konusunda çok kararlıdır ve teknoloji bunu yapmak için kullandıkları birçok araçtan sadece biridir.

- Failin seninle ilgili çok fazla bilgisi olduğunu düşünüyorsan, bu bilgileri cihazlarını veya konumunu izleyerek, çevrim içi hesaplarına erişerek ya da hakkında çevrim içi bilgi toplayarak elde ediyor olabilir. Bunu gerçekleştirmek için birden fazla yol ve yöntem kullanılabilir.

İstersen örneklerle biraz bu konuyu pekiştirelim...

Dijital şiddet türleri teknolojinin ilerlemesiyle sürekli değişmektedir!

En yaygın türler nelerdir?

18

ÇEVRİM İÇİ CİNSEL TACİZ (CYBER/ONLINE SEXUAL HARASSMENT)

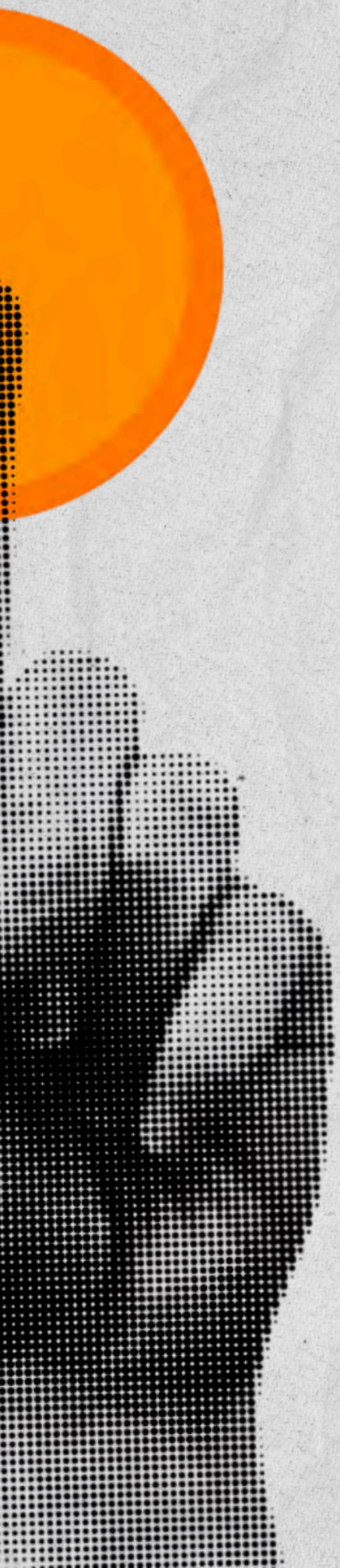
ÇEVRİM İÇİ ISRARLI TAKİP (CYBERSTALKING)

GÖRSEL-ODAKLI CİNSEL TACİZ (IMAGE-BASED ABUSE)

CİNSİYETÇİ NEFRET SÖYLEMİ (GENDER-BASED HATE SPEECH)

Diğer kavramlar nelerdir?

Sahte Taban Mobilizasyonu **(Astroturfing)**, Çevrim içi Kimliğe Bürünme **(Catfishing)**, Çoklu Platform Tacizi **(Cross-Platform Harassment)**, Dijital Teşhir **(Cyberflashing)**, İsim Dayatması **(Deadnaming)**, Dijital Röntgencilik **(Digital Voyeurism)**, Kişisel Bilgilerin İfşası **(Doxing)**, Teknoloji Destekli Ekonomik Şiddet **(Electronically Enabled Financial Abuse)**, Dijital Kışkırtma **(Flaming)**, Cinsiyetçi Trolleme **(Gender-Trolling)**, Cinsiyetçi Dezenformasyon **(Gendered Disinformation)**, Arama Motoru Manipülasyonu **(Googlebombing)**, Çocuğa Yönelik Dijital Tuzak **(Grooming)**,



Etiket İçeriğini Bulandırma **(Hashtag Poisoning)**, Akıllı Cihaz Destekli Taciz **(Internet of Things (IoT) Abuse)**, Çevrim içi İtibarsızlaştırma **(Online Defamation)**, Çevrim içi Kimlik Hırsızlığı **(Online Impersonation)**, Kötücül İçerik Yayma **(Malicious Distribution)**, Kötücül Yazılım Saldırısı **(Malware Attacks)**, Toplu Raporlama **(Mass Reporting)**, Dijital Yıldırma **(Sealioning)**, Dijital Cinsel Şantaj **(Sextortion)**, Dijital Sisleme **(Shadow Banning)**, Sahte Baskınlama **(Swatting)**, Erküre / Eril Hava Sahası / Dijital Erkekçilik Evreni **(The Manosphere)**, Çevrim içi Toplantı Baskını **(Zoombombing)**

Haydi şimdi bunları kavram kartları* şeklinde sıralayalım:

*Bu kavramların Türkçe karşılıkları Kasım 2025'te UN Women ve UNFPA'in çağrısı ile 30'a yakın sivil toplum örgütü temsilcisi ve konunun uzmanları ile dijital şiddet kavramlarını ve türlerini farklı bakış açılarıyla derinlemesine ele alma ve dijital şiddet alanında ortak bir kavramlar sözlüğü geliştirme hedefiyle bir araya geldiğimiz atölye sonucunda ortaya çıktı.

En yaygın biçimlerinden başlayalım

Çevrim içi Cinsel Taciz

CYBER/ONLINE SEXUAL HARASSMENT

NEDİR?

İstenmeyen cinsel ilgi ve cinsel zorlama içerebilen bir taciz biçimi. "Dijital yollarla gerçekleştirilen istenmeyen herhangi bir cinsel davranış" olarak da tanımlanır.[19]

Kullanılan yöntem / araçlar:

- Dijital ortamlarda fiziksel-cinsel şiddetle tehdit etmek, cinsiyetçi şakalar yapmak, bedensel görünüm ya da cinsel deneyimler hakkında yorum yapmak, cinsel içerikli imalı iletiler göndermek, uygunsuz cinsel jestler göndermek, bir kişiden defalarca randevu istemek, bir kişinin cinsiyet kimliği hakkında aşağılayıcı yorumlar yapmak[20]

Örnekler:

- Bir kadın siyasetçinin kadın hakları kampanyasını duyurmasının ardından bir gün içinde binlerce tecavüz / ölüm tehdidi alması
- Kadın oyunculara sosyal medya platformlarından veya mesajlaşma uygulamalarından cinsel içerikli görseller gönderilmesi



Çevrim içi Israrlı Takip

CYBERSTALKING

NEDİR?

Bir kişinin dijital platform ve araçlar kullanılarak tekrarlanan, istenmeyen eylem ve davranışlarla özel olarak hedef alınması.[21] Çoğunlukla çevrim dışı takibin bir uzantısıdır.

Kullanılan yöntem / araçlar:

- Mesajlaşma - sosyal medya platformları, e-posta ve telefon yoluyla tekrar eden rahatsız edici davranışlar
- Casus yazılım, mobil navigasyon, harita uygulamaları veya cihaz hackleme yoluyla kişinin faaliyetlerinin takip edilmesi
- Akıllı ev aletleri (kameralar vb.) aracılığı ile izlenme

Örnekler:

- Bir kişinin eski / şu anki partneri tarafından casus yazılım(lar) yüklenerek telefonunun ve konumunun takip edilmesi
- Bir kişinin çevrim içi ortamda ısrarlı şekilde izlenmesi, ardından fiziksel mekanlarda karşısına çıkılarak tacizin çevrim dışına taşınması

Görsel Odaklı Cinsel Taciz

IMAGE-BASED ABUSE

NEDİR?

Çoğunlukla çevrim içi olarak, mahrem ya da özel görüntülerin / videoların veya cinsel nitelikteki görüntülerin / videoların rıza olmaksızın oluşturulması, manipüle edilmesi ve yayılması ya da bunu yapma tehditlerini kapsar. Bu görüntüler / videolar, görüntüde yer alan kişinin rızasıyla ya da rızası olmadan elde edilmiş olabilir. [22]

Kullanılan yöntem / araçlar:

- Yapay zeka tabanlı araçlarla düzenlenmiş ya da üretilmiş görsel, video veya seslerin birini gerçekte yapmadığı ya da söylemediği şeyleri yapıyor veya söylüyor gibi göstermesi (deepfake*)
- Gizli çekim, çalınan içerik, hesap ele geçirme sonrası elde edilen görüntüleri yayma

Örnekler:

- Eski partnerin elinde olan, rızayla gönderilmiş görüntülerin ayrılık sonrası izinsiz şekilde paylaşmakla tehdit edilmesi
- Bir şarkıcının deepfake ile oluşturulmuş cinsel görüntülerinin itibarsızlaştırma amacı ile çevrim içi ortamda dolaşıma sokulması



Cinsiyetçi Nefret Söylemi

GENDER-BASED HATE SPEECH

NEDİR?

Cinsiyet kimliğine dayalı nefreti yayan, kışkırtan, teşvik eden veya meşrulaştıran ifadeler. [23]

Kullanılan yöntem / araçlar:

- Kadınları cinsel nesneler olarak tasvir eden içeriklerin üretilip yayılması
- Cinsiyetçi ve hakaret içeren yorumların yazılması
- Beden utandırma, cinsiyet kimliği temelli aşağılayıcı klişelerin ve “alay” kültürünün dijital alanlarda kullanımı

Örnekler:

- Bir kadın siyasetçiye yönelik gönderilerde cinsiyetçi ve cinsel şiddet içerikli yorumların temizlenmemesi / kalması
- Spor etkinliklerinde kadın oyunculara yönelik nefret söylemi içeren içeriklerinin üretilmesi

*Yapay zeka tabanlı araçlarla düzenlenmiş ya da üretilmiş görsellerin, videoların veya seslerin birini gerçekte yapmadığı ya da söylemediği şeyleri yapıyor veya söylüyor gibi göstermesi

Diğer kavramlara da sıra ile bakalım:



Sahte Taban Mobilizasyonu

ASTROTURFING

NEDİR?

Taban düzeyinde organik olarak ortaya çıkıp yayılıyormuş gibi görünen ancak gerçekte bir birey, çıkar grubu, siyasi oluşum veya kuruluş tarafından (çoğu zaman birden fazla sahte hesap kullanılarak) üretilen içeriklerin (kötüye kullanım dahil) koordineli bir şekilde yayılması veya güçlendirilmesi.[24]

Kullanılan yöntem / araçlar:

- Sahte / anonim hesaplar üzerinden içerik üretme, etiket (hashtag) kampanyaları ve koordineli yorum yazımı ile platformlarda "yaygın kanaat" izlenimi oluşturma
- Yanıltıcı kampanya mesajlarını belirli etiketlerle paylaşma, aynı anlatıyı farklı mecralara taşıma
- Aynı anlatıyı sosyal medya, forum siteleri ve mesajlaşma kanallarında eşzamanlı dolaşıma sokma

Örnekler:

- Eşitlik savunucusu kampanyalara (örn. kadın hakları kampanyaları) karşı organize şekilde mizojinist içerikler paylaşılması ve "toplum karşı çıkıyor" algısı yaratılması
- #GüvendeDeğilim etiketine, bot hesaplar tarafından "abartıyorsunuz" mesajlarının kopyalanıp yapıştırılması

Çevrim içi Kimliğe Bürünme

CATFISHING

NEDİR?

İnternette sahte bir kimlik / hesap yaratarak (çoğunlukla başkalarına ait fotoğraflar ve onların yaşam öykülerini kullanarak) bir kişiyi duygusal olarak kandırma ve onunla gerçek bir çevrim içi arkadaşlık / romantik ilişki içindeymiş gibi davranmasını sağlamak. Failin hedefi duygusal manipülasyon aracılığıyla para, hediyeler, mahrem görüntüler elde etmek veya daha sonra şantaj yapmak olabilir.[25]

Kullanılan yöntem / araçlar:

- Sahte profil(ler) oluşturma
- Hızlı duygusal yakınlaşma
- Para / hediye / banka hesap bilgisi isteme; ödeme / para gönderme talepleri için sahte acil durumlar üretme
- Bazı durumlarda gerçek bir kişinin hesabını taklit etme veya hackleyip o kişiymiş gibi davranma

Örnekler:

- Flört uygulamalarında sahte bir kimlik kullanarak kendisini varlıklı biri gibi tanıtan bir failin, birden fazla kadının güvenini kazanıp “acil durum” bahanesiyle maddi taleplerde bulunması ve kadınları maddi olarak istismar etmesi

Çoklu Platform Tacizi

CROSS-PLATFORM HARASSMENT

NEDİR?

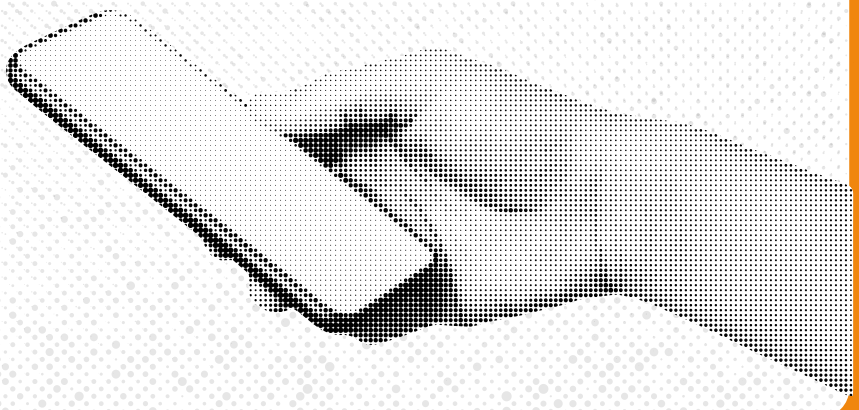
Bir fail ya da fail grubunun, bir kişiyi / kişileri taciz etmek amacıyla birden fazla sosyal medya ve iletişim platformunu eşzamanlı / ardışık ve kasıtlı biçimde kullanması.[26]

Kullanılan yöntem / araçlar:

- Aynı hedefe yönelik farklı sosyal medya platformlarında eşzamanlı saldırılar düzenleme (sayısız yorum yazmak, mesaj atma, etiketleme)
- Her platform yalnızca kendi bünyesindeki tacizi dikkate aldığı için fail(ler)in, her seferinde "tekil olay" izlenimi yaratması

Örnekler:

- Bir kadın gazeteci hakkında X'te başlatılan itibarsızlaştırma kampanyasının, aynı gün senkronize şekilde Instagram yorumlarına, YouTube videolarının altına ve Telegram / WhatsApp gruplarına taşınması
- Bir aktivistin kullanıcı adı hedef gösterilerek Reddit'te konu başlıklarının açılması, TikTok'ta manipüle edilmiş videolar üretilmesi, Discord'da organize olan kullanıcıların Instagram mesajları ve e-postalarla tehdit ve tacizi çok kanallı bir şekilde sürdürmesi



Dijital Teşhir

CYBERFLASHING

NEDİR?

Flört uygulamaları, mesajlaşma uygulamaları, e-posta, sosyal medya platformları veya AirDrop gibi dosya paylaşım uygulamaları üzerinden, alıcının izni olmadan cinsel içerikli fotoğraf veya videoların gönderilmesi. Bu eylem, kişinin mahremiyetini ihlal eder ve çoğu zaman cinsel taciz olarak değerlendirilir.[27]

Kullanılan yöntem / araçlar:

- AirDrop ve Bluetooth üzerinden dosya gönderimi
- Mesajlaşma, e-posta ve sosyal medya platformlarında görüntü paylaşımı
- Görüntülü arama ve canlı yayınlarda görüntü paylaşımı

Örnekler:

- Bir kişinin, flört uygulaması üzerinden iletişim kurduğu bir kadına izni olmadan cinsel içerikli bir fotoğraf göndermesi; kadının mahremiyetinin ihlal edilmesine ve dijital ortamda güvensizlik hissetmesine yol açması
- Toplu taşıma, kafe veya kamusal bir alanda AirDrop gibi bir dosya paylaşım özelliği aracılığıyla çevredeki kadınlara istemedikleri cinsel içerikli görüntülerin gönderilmesi

İsim Dayatması

DEADNAMING

NEDİR?

Hedef alınan kişiye zarar verme amacıyla, kişinin artık kullanmadığı, doğum adını (eski isim) onun rızası ve tercihleri dışında kasıtlı olarak ifşa etme veya kullanmak. Özellikle trans ve non-binary bireylerin kendi tercihiyle değiştirdiği isimlere saygı gösterilmemesi veya bu isimlerin kötü niyetle yayılmasıdır.[28]

Kullanılan yöntem / araçlar:

- Sosyal medya platformlarında, haber siteleri veya forumlarda kişinin yeni adını görmezden gelip eski adıyla etiketleme veya başlıklandırma
- Etiket (hashtag) saldırıları, tekrar eden yanıt / yorum yığını ile kişinin eski adının yoğunluklu bir şekilde dolaşıma sokulması

Örnekler:

- Bir araştırmacının, akademik yayınlarında artık kullanmadığı ismin kaldırılması için talepte bulunmasına rağmen yayınevlerinin bu talebi dikkate almaması ve eski ismin dolaşımda kalmaya devam etmesi.
- Bir sanatçının kendi seçtiği isimle kamuya açık şekilde var olmasına rağmen, medya kuruluşlarının haberlerde eski ismini kullanmayı sürdürmesi.

Dijital Röntgencilik

DIGITAL VOYEURISM

NEDİR?

Bireylerin bilgisi veya izni olmadan gizlice görüntülerinin çekilmesi. Daha uzun bir takip / istismar örüntüsünün parçası olabilir.[29]

Kullanılan yöntem / araçlar:

- Gizli kamera, akıllı telefon, kalem / gözlük / kumanda görünümlü cihazlar vb. ile rıza dışı fotoğraf / video çekme
- Bir kişinin elbisesinin ya da eteğinin altından görüntü alma (upskirting)
- Fark ettirmeden bir kişinin rıza dışı cinsel çağrışımlı fotoğrafını çekme (creepshot)

Örnekler:

- Bir alışveriş mağazasının deneme kabinine yerleştirilen gizli kamerayla müşterilerin kıyafet değiştirirken kayda alınması
- Okul soyunma odasında akıllı telefonla fark ettirmeden video çekilip kapalı mesaj gruplarında paylaşılması

Kişisel Bilgilerin İfşası

DOXING

NEDİR?

Doxing, kişinin kimliğini ifşa edecek bilgilerin izni olmadan toplanması ve çevrim içi olarak paylaşılması. Bir kişinin ev ve e-posta adresleri, telefon numaraları, işyeri ve aile üyelerinin iletişim bilgileri ya da çocuklarının fotoğrafları ve gittikleri okul gibi özel, kişisel, hassas bilgilerin kamuya açıklanmasını içerir.[30]

Kullanılan yöntem / araçlar:

- Ev / iş adresi, telefon, konum bilgisi ve çocuklarının okulu gibi bilgileri kişinin rızası olmadan yayınlama
- Özel e-posta / mesaj dökümleri, kişisel fotoğraflar veya mahrem detayları paylaşarak itibar zedeleme ve utandırma
- De-anonimleştirme (anonimliği kırma), takma adlı / anonim kişinin kimliğini, eski / yeni paylaşımlarını ortaya çıkarma

Örnekler:

- Bir kadın siyasetçinin çocuğunun fotoğrafının ve okulunun adının paylaşılması; e-posta ve telefonuna şiddet içerikli tehditler gelmesi
- Bir kadın oyuncunun mesaj arşivlerinden alınan özel yazışma ve eski fotoğrafların yayınlanıp "itibarsızlaştırma" kampanyası yürütülmesi

Teknoloji Destekli Ekonomik Şiddet

ELECTRONICALLY ENABLED FINANCIAL ABUSE

NEDİR?

Genellikle yakın partner şiddetine maruz kalan bir kadın üzerinde, mali baskı uygulamak için internet ve diğer teknoloji biçimlerinin kullanılması.[31]

Kullanılan yöntem / araçlar:

- İnternet bankacılığı / parola sıfırlama üzerinden ortak / kişisel hesaplara erişimi kısıtlama; hesap hareketlerini ve harcamaları sürekli izleme
- Kart / ödeme limitlerini tek taraflı düşürme, çevrim içi alışveriş ve fatura ödemelerini engelleme, dijital cüzdan ve ödeme uygulamalarını denetleme
- Adına izinsiz kredi çekme, abonelik açma, sahte borç kaydı oluşturma, kredi puanını düşürme
- Kişisel verileri çalıp finansal işlemlerde kullanma; iki aşamalı doğrulama kodlarını ele geçirerek işlem yapma

Örnekler:

- Failin, kadının çevrim içi alışverişlerini engelleyerek her harcamayı kendi iznine bağlaması
- Failin, eşi adına internet üzerinden kredi başvurusu yapıp kadını borçlandırması

Dijital Kışkırtma

FLAMING

NEDİR?

Çevrim içi ortamda doğrudan hakaret, küfür veya saldırgan ifadeler içeren paylaşımlar yapılması. Cinsiyetçi Trolleme'den (Gender Trolling) farklı olarak, hedefi anlaşmazlık yaratmaktan ziyade doğrudan düşmanca ve provoke edici bir dil kullanmaktır. Genellikle forumlar, sosyal medya ve anonim platformlar üzerinden gerçekleşir ve kullanıcıların anonimliği saldırgan davranışların ortaya çıkmasına zemin hazırlar.[32]

Kullanılan yöntem / araçlar:

- Sosyal medyada, forumlarda veya bu platformların yorum bölümlerinde doğrudan hakaret ve küfürlü mesaj gönderme
- Anonim hesap veya sahte profiller üzerinden saldırgan paylaşımlar yapma
- Provoke edici, tehditkar veya aşağılama amaçlı içerikler planlama

Örnekler:

- Kadına yönelik şiddetle ile ilgili paylaşım yapan bir akademisyenin, anonim hesaplar tarafından doğrudan hakaret, küfür ve tehdit içeren mesajlarla hedef alınması, kullanıcının paylaşımlarını silmek zorunda kalması ve çevrim içi görünürlüğünü azaltması
- Çevrim içi tartışma platformlarında siyasi görüş bildiren kadın kullanıcıların, anonim hesaplar tarafından sürekli hakaret, küçültücü ifadeler ve tehdit mesajlarıyla hedef alınarak tartışmalara katılımlarının engellenmeye çalışılması ve birçok kullanıcının güvenlik kaygısıyla geri çekilmek zorunda kalması

Cinsiyetçi Trolleme

GENDER TROLLING

NEDİR?

Kadınların, toplumsal cinsiyet eşitliği veya tartışmalı konularda görüş bildirmeleri durumunda, salt kadın olmalarından dolayı çevrim içi ortamda hedef alınarak sindirilmeye, itibarsızlaştırılmaya veya dijital alanlardan çekilmek zorunda bırakılmaya çalışıldığı trolleme biçimi. "Şaka" veya "mütevazı eleştiri" kisvesi altında gösterilmeye çalışılsa da temelinde cinsiyete dayalı düşmanlık, küçümseme ve güç gösterisi vardır.[33]

Kullanılan yöntem / araçlar:

- Küçük düşürücü yorumlar, hakaret, itibar zedeleme
- Koordineli trol saldırıları
- Doğrudan tehdit ve taciz

Örnekler:

- Kadın gazetecilerin, özellikle siyasi haberler, kadın hakları veya toplumsal cinsiyet eşitliği üzerine paylaşımlar yaptığında, toplu ve organize trol saldırılarına maruz kalması
- Oyun kültüründe kadın temsilini eleştiren feminist bir medya eleştirmeninin, hazırladığı içerik sonrası organize trol grupları tarafından yoğun hakaret, itibarsızlaştırma ve tehdit içeren saldırılara maruz bırakılarak dijital alandan çekilmeye zorlanması



Cinsiyetçi Dezenformasyon

GENDERED DISINFORMATION

NEDİR?

Kadınlara ve özellikle kadın liderlere karşı, çoğu zaman belirli bir düzeyde koordinasyonla yürütülen, kadınları kamusal alana katılmaktan caydırmayı ve belirli siyasi ve toplumsal gündemleri teşvik etmeyi amaçlayan, cinsiyete dayalı yanlış veya yanıltıcı anlatıların kullanılması.[34]

Kullanılan yöntem / araçlar:

- Cinsiyetçi kalıp yargıların ("yetersizlik", "duygusallık", "ahlaksızlık" vb.) sistematik yayılımı
- Cinsiyet kimliği ile birlikte ırk, etnisite, engellilik vb. üzerinden yanıltıcı anlatıların yayılması

Örnekler:

- Bir kadın siyasetçiyi "duygusal / yetersiz" göstermek için koordineli sahte haberler ve manipüle edilmiş görsellerinin dolaşıma sokulması
- Kadın gazeteci / aktiviste yönelik, özel hayatına dair uydurma iddiaların bot ağlarıyla "trend topic" (TT, trend konu) yapılması ve eşzamanlı olarak tehditkar yorumların yazılması



Arama Motoru Manipülasyonu

GOOGLE BOMBING

NEDİR?

Bir kişi veya kurumun çevrim içi itibarını zedelemek amacıyla, arama motoru sonuçlarının manipüle edilmesi. Bu yöntem, belirli internet sitelerine çok sayıda bağlantı (backlink) verilerek, o sayfanın alakasız veya olumsuz arama terimleriyle ilişkilendirilmesini ve aramalarda en üstte çıkmasını sağlar.[35]

Kullanılan yöntem / araçlar:

- Arama motoru algoritmalarını manipüle edecek şekilde bağlantı ağı kurma
- Hedefin adıyla olumsuz içerikleri ilişkilendirme
- Topluluklar veya bot hesaplar aracılığıyla koordineli bağlantı paylaşımı yapma

Örnekler:

- Bir arama motorunun aramaları otomatik tamamlama işlevinde, bir siyasetçinin eşi ile ilgili arama yapıldığı zaman, adının yanında cinsel içerikli kavramların belirmesi

Çocuğa Yönelik Dijital Tuzak

GROOMING

NEDİR?

Çocuğu cinsel istismar veya çocuk ticaretine sürüklemek amacıyla dijital araçların kullanılması.[36]

Kullanılan yöntem / araçlar:

- Oyunlar, doğrudan mesajlar, yorumlar, kapalı gruplar üzerinden iletişim, yaş / kimlik gizleme
- Aile / arkadaşlardan uzaklaştırma, yalnız ve gizli konuşmayı talep etme
- Mahrem görsel / video isteme, rıza dışı paylaşım tehdidi

Örnekler:

- Bir failin, 13 yaşındaki kullanıcıyla oyunda tanışıp haftalarca doğrudan mesajlarla “gizli” konuşmalar yürütmesi, ardından mahrem görüntü istemesi ve “söylersen başın belaya girer” diye tehdit etmesi
- Sosyal medyada “yaşıt” gibi davranan yetişkinin, çocuğu / ergeni platform dışına (şifreli mesajlaşma) taşıyıp hediye / vaatlerle görüntü talep etmesi

Etiket İçeriğini Bulandırma

HASHTAG POISONING

NEDİR?

Kadın haklarını desteklemek, deneyim paylaşımına alan açmak için oluşturulan bir etiketin altındaki içeriklerin tam tersi söylemlerle doldurulması.[37]

Kullanılan yöntem / araçlar:

- Kadınlara alan açan, seslerini duyurması için kullanılan etiketleri bulmak
- Bu etiketleri domine edecek kadar içerik yayınlamak

Örnekler:

- #TakeBackTheTech ve #ImagineaFeministInternet gibi feminist hashtag'lerin bu kampanyaları "yok etmek" amacıyla koordine bir şekilde yayınlanan kadın düşmanı mesaj ve dijital görsellere boğulması
- Kadınların cinsiyetçi şiddet deneyimlerini paylaşmak için kullandığı #YesAllWomen etiketinin, bazı erkek kullanıcılar tarafından kadınların anlatılarını küçümseyen, alaycı ve cinsiyetçi yorumlar eklemesi

Akıllı Cihaz Destekli Taciz

INTERNET OF THINGS (IOT) ABUSE

NEDİR?

Failin akıllı ev cihazları, giyilebilir teknolojiler ve bağlı ev aletlerini kullanarak kişi üzerinde kontrol kurma eylemi. Kişinin günlük yaşamını izlemek, manipüle etmek ve psikolojik baskı oluşturmak amacıyla gerçekleştirilir.[38]

Kullanılan yöntem / araçlar:

- Akıllı termostatlar aracılığıyla evin sıcaklık seviyesinin kontrol edilmesi
- Akıllı cihazlar aracılığıyla kişinin günlük aktivitelerinin izlenmesi
- Sesli asistan ve diğer bağlı cihazlar üzerinden konuşmaların dinlenmesi

Örnekler:

- Giyilebilir bir sağlık takip cihazı kullanan kadının eski eşinin, cihazın verilerine erişim sağlayıp kadının sağlık durumu hakkında izinsiz bir şekilde bilgi elde etmesi
- Eski eşinin akıllı ev sistemine izinsiz erişim sağlayarak, evdeki iPad aracılığıyla kadının konuşmalarının dinlenmesi

Çevrim içi İtibarsızlaştırma

ONLINE DEFAMATION

NEDİR?

Bir kişi ya da oluşum hakkında yanlış veya çarpıtılmış bilgilerin internet üzerinden yayılması ve bu yolla itibarının zedelenmesi. Genellikle bir kişiyi / oluşumu küçük düşürme, tehdit etme, itibarsızlaştırma, sindirme veya cezalandırmayı amaçlar. Çoğu zaman kamusal alanda daha görünür olan kadın siyasetçi, gazeteci, aktivist ve sanatçılar hedef alınır.[39]

Kullanılan yöntem / araçlar:

- Kasıtlı olarak üretilen yanlış veya çarpıtılmış bilgilerin sosyal medya platformlarında paylaşılması
- Değiştirilmiş görüntü, video veya belgeler üzerinden karalama kampanyası yürütülmesi
- Yanlış / asılsız içeriklerin daha geniş kitlelere ulaştırılması için "trend topic" (TT, trend konu) yapılması (hashtag'ler üzerinden çoklu paylaşım)

Örnekler:

- Bir gazeteci hakkında sosyal medyada koordineli şekilde iftira kampanyası yürütülmesi ve onlarca sosyal medya hesabının aynı anda yanlış bilgi paylaşması
- Bir aktivistin itibarsızlaştırılması için manipüle edilmiş görsellerin yayılması

Çevrim içi Kimlik Hırsızlığı

ONLINE IMPERSONATION

NEDİR?

Kişiye iftira atmak, onu itibarsızlaştırmak ya da daha fazla istismarı tetiklemek amacıyla sahte bir sosyal medya hesabı oluşturmak. Aynı zamanda birini, rızası olmadan yanlış biçimde temsil etmek ve içerik oluşturmak.[40]

Kullanılan yöntem / araçlar:

- Birinin kimliğini kullanarak sosyal medya hesapları oluşturma
- Yapay zekayı kullanarak deep fake video veya görüntüler oluşturma
- Kişinin kimliğine zarar verecek içerik paylaşma

Örnekler:

- Bir erkeğin, bir kadın adına cinsel içerikli bir sitede, kadının kişisel bilgilerini içeren detaylı bir profil açması
- Seçim dönemlerinde kadın siyasetçilerin adına sahte hesapların açılıp, kampanyaları ile bağdaşmayan söylemlerin dolaşıma sokulması

Kötücül İçerik Yayma

MALICIOUS DISTRIBUTION

NEDİR?

Kötü niyetli dağıtım, kişinin ve / veya kurumların itibarını zedeleyici materyali, örneğin mahrem fotoğraf / videolarını, dağıtmak için teknoloji temelli araçlarının kullanılması.[41]

Kullanılan yöntem / araçlar:

- Birine ait verilerin rızası dışında kötü amaçla dağıtılması
- Kadınların destek mekanizmalarında bulunan verilerin ele geçirilmesi
- Sosyal medya platformları üzerinden kişisel bilgilerin paylaşılması

Örnekler:

- Erkek üyelerden oluşan kapalı bir Facebook grubunda, üyelerin eşlerinin ve kız arkadaşlarının izinsiz çıplak fotoğraflarını paylaşması
- Kürtaj hizmeti sunan bir merkezin elindeki kişisel verilerin, bu hizmetten faydalanan kadınlara yönelik şiddete çağrıda bulunmak için dağıtılması

Kötücül Yazılım Saldırısı

MALWARE ATTACKS

NEDİR?

Kullanıcının, içinde kötü niyetli bir yazılım barındıran bir e-posta ya da mesajdaki bağlantıya tıklaması, bir eki açması ya da bir internet sitesini ziyaret etmesi sonucu cihazına kötü niyetli yazılım gönderilmesi / bulaşması. Bu kötü niyetli yazılımları barından içerikler genellikle resmi bir e-posta adresinden, bir tanıdıktan ya da iş arkadaşından gelmiş gibi görünür.[42]

Kullanılan yöntem / araçlar:

- E-posta ile gelen ekstreler / faturalar
- Sohbet uygulamaları üzerinden paylaşılan indirim mesajları
- İnternet sitelerine yüklenmiş kötü niyetli yazılımlar

Örnekler:

- -Bir kadın siyasetçinin, aday olduğu seçim döneminde açtığı internet sitesine kötü niyetli bir yazılım yüklenmesi ve siteyi ziyaret eden herkesin cihazına virüs bulaşması
- Arkadaşının geçen yaz çektiği fotoğrafları kendisi ile paylaştığını söyleyen bir e-posta alan kadının bağlantıya tıklayıp bilgisayarındaki bütün bilgileri çaldırması



Toplu Raporlama

MASS REPORTING



NEDİR?

Ağırlıklı olarak Instagram olmak üzere X'te (eski adıyla Twitter) de gerçekleşebilen, bir hesabın ya da bir içeriğin sistematik ve toplu olarak rapor edilmesi. Genellikle raporlama belirli bir grup tarafından kullanıcının sözünün geniş kitlelere ulaşmaması için gerçekleştirilir ve raporlamaların anlamlı / geçerli bir sebebi yoktur.[43]

Kullanılan yöntem / araçlar:

- Platformlardaki şikayet mekanizmaları
- Koordineli troller

Örnekler:

- Koordineli trollerin bir hesabı ya da içeriği, aralarında paylaşıp şikayet mekanizmalarını kullanarak aynı anda raporlaması

DİJİTAL ŞİDDETE NOKTAYI KOY!

Dijital Yıldırma

SEALIONING

NEDİR?

Karşı tarafı bunaltmak veya kışkırtmak amacıyla, çoğu zaman temel ve kolayca bulunabilecek bilgiler ya da ilgisiz noktalar üzerinden ısrarlı sorgulama ve karşı tarafı yanıt vermek zorunda bırakma. Motivasyon; karşı tarafın enerjisini, sabrını tüketmek ve sinirini zorlamak, bir yere varmayan tartışmalarda ekran görüntüsü alıp paylaşacak malzeme yaratmaya çalışmak.[44]

Kullanılan yöntem / araçlar:

- Herkese açık sosyal medya platformlarında karşı tarafı hiçbir yere varmayan tartışmaların içine çekmek

Örnekler:

- Bir kadın gazeteci, toplumsal cinsiyet eşitliğiyle ilgili X'te bir içerik yayınladığında bazı kullanıcıların "Ama tam olarak neyi kastediyorsunuz?", "Kadınlara eşit hak verilmiyor derken hangi ülkeden bahsediyorsunuz?", "Bana istatistik gösterebilir misiniz?" gibi masum görünen ama kişiyi sonsuz bir döngüye sokan sorular yöneltmesi
- Feminist bir medya eleştirmeninin taciz ile ilgili bir içerik paylaştığında yüzlerce kez "Gerçekten kanıtın var mı?", "Sadece merak ediyorum, neden erkekler de tacize uğramıyor diyorsun?", "Feminist olmanın tam olarak ne anlama geldiğini açıklar mısın?" gibi "sözde mantıklı" sorulara maruz kalması

Dijital Cinsel Şantaj

SEXTORTION

NEDİR?

Bir kişinin başka birine ait cinsel bir görüntüye sahip olması ya da sahip olduğunu iddia etmesi ve bunu, o kişiyi istemediği bir şeyi yapmaya zorlamak için kullanması.[45]

Kullanılan yöntem / araçlar:

- Failin, daha önce rızayla paylaşılmış ya da hack / dolandırıcılıkla elde ettiği görüntüleri yayma tehdidi
- Deepfake veya manipüle edilmiş görüntüleri varmış gibi göstererek tehdit etme
- "Bilgisayarını / kameranı hackledim, çıplak fotoğraflarını çektim" diyerek tehdit etme
- Eski / şu anki partnerin daha önce paylaşılan görüntüleri tehdit aracı olarak kullanması

Örnekler:

- Bir failin, kişinin bilgisayarını hacklediğini ve çıplak görüntüler elde ettiğini iddia ederek para talep etmesi
- Boşanma aşamasında eski eşin elindeki cinsel içerikli görüntülerin "Ailene gönderirim" diyerek boşanmamak için tehdit unsuru olarak kullanılması

Dijital Sisleme

SHADOW BANNING

NEDİR?

Ağırlıklı olarak Instagram olmak üzere X'te (eski adıyla Twitter) de gerçekleşebilen, hesabınızın ya da bir içeriğinizin sistematik ve toplu olarak rapor edilmesi sonucu içeriklerinizi sadece takipçilerinizin ya da takipçilerinizin kısıtlı bir bölümünün görebilmesi. Buna maruz kalan kullanıcıların bunu doğrudan anlaması çok olası değildir, etkileşim sayılarındaki belirgin düşüş bunun göstergelerindendir.[46]

Kullanılan yöntem / araçlar:

- Platformlardaki şikayet mekanizmaları
- Koordineli troller

Örnekler:

- Koordineli trollerin bir hesabı ya da içeriği, aralarında paylaşıp şikayet mekanizmalarını kullanarak aynı anda raporlaması sonucu kullanıcının içeriklerinin takipçilerinin büyük bir kısmına ulaşamaması



Sahte Baskınlama

SWATTING

NEDİR?

Kolluk kuvvetlerine, hedefin evinde veya işyerinde gerçekleşen ve kolluk kuvveti müdahalesi gerektirdiği iddia edilen bir olayı aktaran sahte telefon araması ya da çevrim içi ihbar sonucu tam teçhizatlı bir polis biriminin hedefin adresine gönderilmesini sağlama.[47] Adını militarize teknikler, ekipman ve ateşli silahlar kullanan ABD polis birimi "SWAT"tan (Special Weapons and Tactics) alır.[47]

Kullanılan yöntem / araçlar:

- Telefon araması
- Çevrim içi ihbar yöntemleri

Örnekler:

- Evinde bir cinayet gerçekleştiğine dair yapılan bir telefon ihbarı sonucunda göz önünde olan bir oyuncunun evinin basılması
- Çevrim içi ihbar yöntemleri kullanılarak bir influencer'ın sabahın erken saatlerinde 30'a yakın silahlı polis ekibi tarafından uyandırılıp evinin basılması

Erküre / Eril Hava Sahası / Dijital Erkekçilik Evreni

THE MANOSPHERE

NEDİR?

Çeşitli "erkek haklarını(!)" ve çıkarlarını savunan, aynı zamanda kadın düşmanı ideolojileri, anti-feminist ve cinsiyetçi inançları teşvik eden çevrim içi erkek topluluk ağları.[48]

Alt gruplar:[49]

- **Involuntary celibates (incel'ler):** Cinsel ilişki kurma konusundaki algılanan yetersizlikleri (kendi düşünceleri) nedeniyle kadınlara yönelik mizojinist (kadın düşmanı) suçlamalarda bulunan erkekler.
- **Men's Rights activists (MRas):** Sıklıkla akademik bir tonla, feminizmin ve kadın -oy hakkı, eğitim, liderlik pozisyonları- haklarının erkekleri dezavantajlı duruma düşürdüğünü iddia eden erkekler.
- **"Pick up artist"ler (PUa'lar):** Cinsel rıza / onay kavramı ile alay eden erkekler.
- **"Men Going Their Own Way" (MGTOW) hareketi:** Toplumun erkeklerin aleyhine kurgulandığını ve kadınlardan, hatta bütünüyle ana akım toplumdan uzak durmanın en iyisi olduğunu öne süren erkekler.

Örnekler:

- Çevrim içi incel forumlarında kadınlara yönelik şiddet çağrılarının artması ve bazı bireylerin bu ideolojilerden etkilenerek şiddet eylemleri gerçekleştirmesi
- Sosyal medya platformlarında PUA (cinsel rıza / onay kavramlarıyla alay edenler) içerik üreticilerinin, erkeklere kadınların "Hayır'ı yok saymayı" öğreten videolar yayması
- Politik tartışmalarda MRAs ("erkek hakları aktivistleri" gruplarının, kadın liderleri hedef alarak feminizmi "toplumsal çöküş" olarak tanımlaması

SÖYLEMLER:

KIRMIZI HAP İDEOLOJİSİ VEYA "REDPILLED" OLMAK

Dünyanın erkeklere kıyasla kadınları kayırdığı bir gerçekliğe uyanmak anlamına gelir. 1999 yapımı bir bilimkurgu aksiyon filmi olan Matrix filmine gönderme yaparak, aksini düşünenlerin mavi hapı aldığı ima edilir.

AWALT: "ALL WOMEN ARE LİKE THAT" (TÜM KADINLAR ÖYLEDİR):

Kadınları kalıplaştırmak için kullanılır.

"FEMOİD" - "FHO"LAR (FEMALE HUMANOİD ORGANİSM)

Kadınların yalnızca erkeklerden aşağı değil, insanlardan da aşağı olduğunu ima eden hakaret içerikli bir terim.

"HYPERGAMOUS"

Kadınların, kendilerinden daha yüksek statü, zenginlik veya görünüşe sahip erkeklerle partner olmayı tercih ettiği konusunda oluşmuş yargı sonucu, erkeklerle "yukarı doğru" evlenmeye takıntılı olduklarını ima etmek için aşağılayıcı biçimde kullanılan terim.

Çevrim içi Toplantı Baskını

ZOOMBOMBING

NEDİR?

Zoombombing, istenmeyen ve davetsiz bir kullanıcı ya da kullanıcı gruplarının çevrim içi toplantıya sızıp / toplantıyı basıp kesintiye uğratması. Bu kesinti, davetsiz kişilerin toplantı sahibinin izni olmadan isimlerini müstehcen kelimelerle değiştirmesi, toplantının izinlerindeki açıklardan faydalanıp görüntü / ses paylaşarak cinsiyetçi, saldırgan ya da nefret söylemi içeren içerikler paylaşması ile gerçekleşir.[50] Adını COVID-19 pandemisi sırasında çoğu etkinliğin Zoom adlı toplantı platformuna taşınmasından alır.[51]

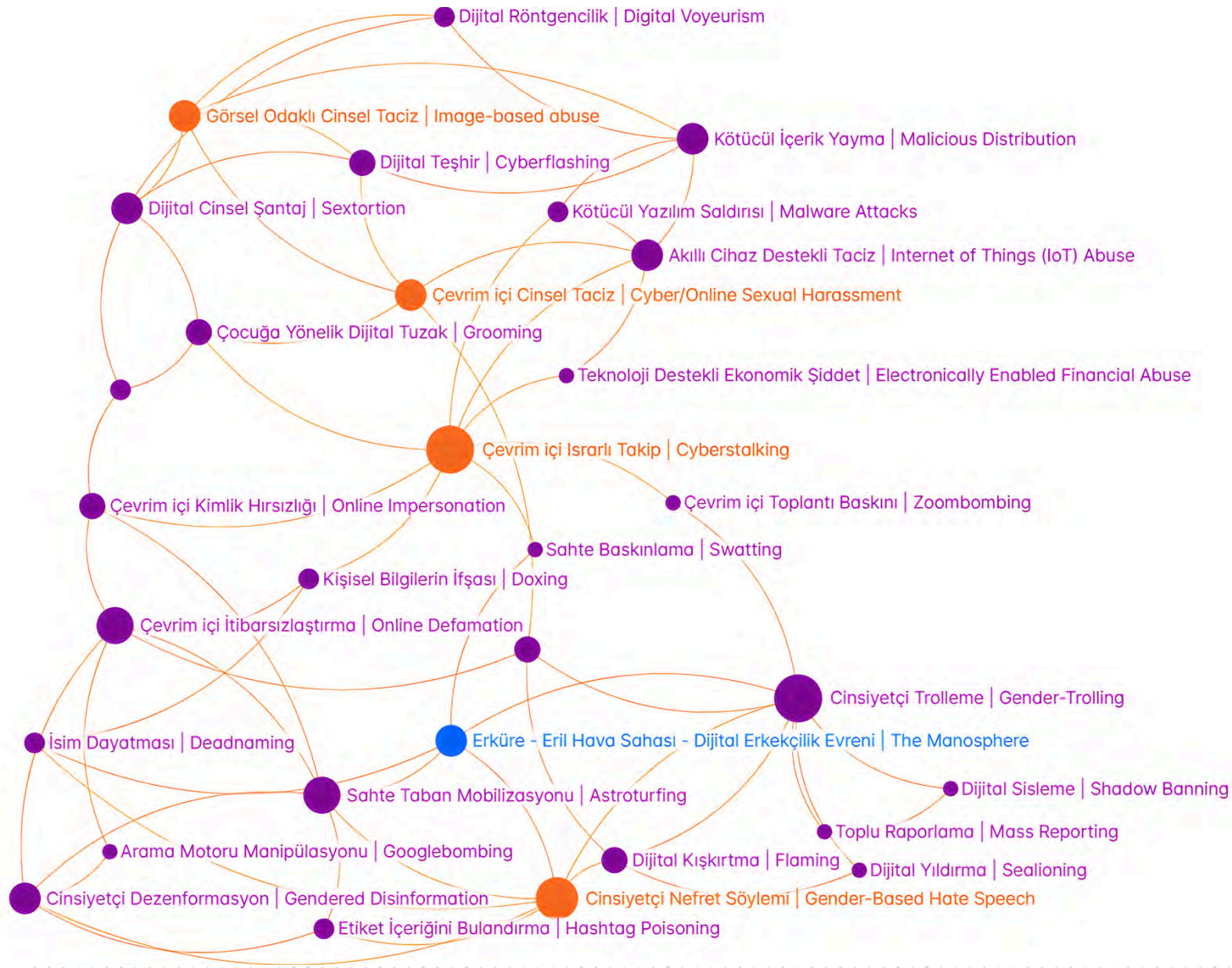
Kullanılan yöntem / araçlar:

- İzinsiz görüntü ve / veya ses paylaşımı
- Kullanıcı adını değiştirme
- Toplantının kontrolünü ele geçirme

Örnekler:

- Bir üniversitede bir kadın profesörün spor ile ilgili konuşmak için informel bir toplantı düzenlemesi ve toplantı başladıktan kısa bir sonra 5-6 kullanıcının toplantıya girip müstehcen görüntüler göstermesi, profesörün toplantı üzerindeki kontrolünü tamamen kaybetmesi

Tüm bu kavramlar aynı zamanda birbiri ile bağlantılı!
Aralarındaki bağlantıyı daha iyi anlamak için
bu bağlantıya tıkla ya da QR kodu okut!



Dijital şiddetin etkileri neler?

Dijital şiddet, ataerkil rolleri, normları ve yapıları pekiştirerek toplumsal cinsiyet eşitliğini güçleştirmekte ve Sürdürülebilir Kalkınma Amaçları'nın 5. hedefi olan 'toplumsal cinsiyet eşitliğini sağlamak ve tüm kadınlar ile kız çocuklarını güçlendirmek' amacına ulaşmanın önünde önemli bir engel oluşturmaktadır.

Dijital şiddete maruz kaldığımızda öfke, şaşkınlık çaresizlik, güçsüzlük, kendi güvenliğimizden endişe, korku ve üzüntü hissedebilir, aile ve arkadaşlarımızın duymasından endişe edebiliriz.

Yaşadığımız şiddeti önemsizleştirebilir, kendimizi suçlayabilir ve olanları değiştirmek için yapabilecek hiçbir şey olmadığı inancına kapılabiliriz.

Yaşadığımız kafa karışıklığı, ne yapacağımızı bilememe hali çok normal.

Özellikle güvenlik endişesi veya belirsizlik nedeniyle yaşanılan şiddeti bir süre kimseyle paylaşmamak ya da saklama ihtiyacı duymak da yaygın ve anlaşılır bir tepkidir.

Dijital şiddete maruz kalanların sosyal hayatları ve iş yaşamları sıklıkla etkilenmekte, hareketlilikleri sınırlanmaktadır. Kadınlar genellikle dijital şiddet sonucu korku, endişe ve depresyon yaşabilir; ki bu da sosyal medya hesaplarını kapatıp çevrim içi alanlardan çekilmelerine yol açabilir.

Bir sosyal medya hesabının kapatılması küçük bir şey gibi görünebilir. Ancak, bu özellikle kadınların ve kız çocuklarının dijital alanlardan çekilmesi anlamına geliyor. Dijital şiddet, kadınları çevrim içi ortamlarda susturmayı hedefler. Aynı zamanda kamusal ve siyasi yaşama, demokratik süreçlere ve liderlik rollerine katılımlarını azaltmak için kullanılır.

Kamusal, özel ve dijital alanlarda kendini güvenli ve özgür hissetmek ve ifade edebilmek hepimizin hakkı.

Neler yaparak kendini güvende tutabilirsin?

Çevrim içi platformlarda hedef olmak, utanmana, güvensiz hissetmene, kendini suçlamana ve işlerin tamamen kontrolden çıktığını hissetmene neden olabilir. Bazen herhangi bir şey yapmak da istemeyebilirsin. Ama kendini suçlamadan alabileceğin önlemler var.

Bunlardan bazıları:

Kendine güven!

- Kendine güvenmekle ve yaşadıklarının şiddet olduğunu tanımlamakla başlayabilirsin.
- Unutma: **Suçlu olan sen değilsin!** Kendini suçlamaman gerektiğini ve şiddetin hiçbir gerekçesi olamayacağını sürekli kendine ve çevrende benzer durumlara maruz kalanlara hatırlat.
- Yaşanılan şiddet sonrası hissedilenler, ihtiyaçlar ve yapılacaklar kişiden kişiye değişebilir!

Güvendiğin biri ile paylaşabilirsin, danışmanlık alabilirsin.

- Bir arkadaşın, ailenden biri veya güvendiğin başka biriyle neler olduğunu ve bunun seni nasıl hissettirdiğini konuşabilirsin.
- Güvendiğin kişilerin kim olduğunu yine en iyi sen bilirsin.
- Konunun uzmanı psikolog, avukat ya da bilişim uzmanlarından danışmanlık alabilirsin.
- Kadın danışma merkezlerini de arayabilirsin.



Seni iyi hissettiren bir şey yap!

Dijital ortamlarda bulunmak seni zorluyor ya da zaman zaman yoruyorsa, kendine her gün küçük bir alan açabilir ve çevrim içi dünya ile bir süre için mesafe koyabilirsin.

Kendi kendine ya da arkadaşlarınla sevdiğin bir şeyler yapabilirsin. Ya da ekran süreni azaltmakla başlayabilirsin.

Kanıt topla!

Öncelikle yaşadığın dijital şiddeti **belgele.** Yasal yolları işletmek istersen bu belgelere ihtiyacın olacak. Ayrıca bu belgeler durumunu görmene ve güvenlik planlaması yapmanda sana yardımcı olabilir.

Ekran görüntülerini almayı ve silinme ya da yok edilme riskine karşı **yedeklemeyi** unutma. E-Tespit yapabilirsin, belgelemek istediğin içeriğin tespitini gerçekleştirmek için Türkiye Noterler Birliği'nin **E-Tespit Portal** sayfasını kullanabilirsin.



- Yasal süreçleri öğrenmek için konu ile ilgili çalışan avukatlar ile Baroların Kadın Danışma Merkezleri / Komisyonları ile görüşebilirsin.
- Polis-Jandarma birimlerine veya adli makamlara suç duyurusunda bulunabilirsin. Öncesinde ilgili tüm bilgi ve belgeleri derlemeyi unutma.
- İlgili kurumlara bildirimde bulunmaya karar verirsen güvendiğin bir kişiden sana süreç boyunca eşlik etmesini iste.
- Fail iş arkadaşınsa bunu çalıştığın kurumun başvuru mekanizmasına (etik kurul vb.) bildirebilirsin. Gizliliğinin korunması çok önemli, bunu talep edebilirsin.
- Unutma, kişisel verilerinin ve özel hayatının gizliliğinin korunmasını istemek temel haklarındandır.

Dijital şiddet, suç teşkil eden örnekleri içinde barındırır. Ulusal ve uluslararası mevzuatta toplumsal cinsiyete dayalı dijital şiddet ile **mücadelede kullanabileceğin mekanizmalar** yer almakta:

Uluslararası Sözleşmeler:

- Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşmesi (CEDAW)
- Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi)

Ulusal Mevzuat:

- 6284 Sayılı Ailenin Korunması ve Kadına Karşı Şiddetin Önlenmesine Dair Kanun
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- Kişisel Verilerin Korunması Kanunu
- Türk Ceza Kanunu

Çevrim içi Başvurabileceğin Yerler:

- https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu
- https://ihbar.ng112.gov.tr
- Kadın Destek Uygulaması (KADES)
- Vodafone Uygulaması (Kırmızı Işık)
- UNFPA Uygulaması (AMBER)

Başvurabileceğin kurumlar:

- Polis Merkezleri, Jandarma Karakolları
- Şiddet Önleme ve İzleme Merkezi (ŞÖNİM)
- Adli Makamlar (Cumhuriyet Başsavcılığı, Aile Mahkemeleri ve Adli Yardım Merkezleri)
- Kadın Danışma Merkezleri
- Baroların Kadın Danışma Merkezleri

Arayabileceğin Acil Telefon Hatları:

- **112** Acil Çağrı Merkezi (Polis, Jandarma,Sağlık Desteği)
- Alo **183** 7/24 Şiddetle Mücadele Hattı (İşitme ve Konuşma Engelliler İçin - 0549 381 01 83)
- Aile içi Şiddet ve Yardım Hattı **0212 656 96 96 - 0549 656 96 96**
- Türkçe dışında bir dil konuşuyorsan **157** Yabancılar İletişim Merkezi

Dijital güvenliğin için yapabileceğin o kadar çok şey var ki, unutma güç sende!

Dijital dünyada kontrolü elimize alıyoruz!

Dijital platformlarda hem kendini hem de bütün kullanıcıları güvende tutmak için yapabileceklerin var.

Biraz zaman ayırıp dijital platformları herkes için güvenli hale getirmeye çalışmak mümkün!

PLATFORMU TANIYOR MUSUN?



Öncelikle kullandığın dijital platformların taciz ve şiddet konularındaki tutumuna dair bilgi sahibi olman gerek.

Platformları kullanmaya başlamadan önce platformların bu konudaki bölümlerine göz atarsan o platformun seni ne derece koruyacağını ya da şiddet ve tacize maruz kaldığında neler yapmayı taahhüt ettiğini öğrenebilirsin.

O platformda olup olmama kararını da bu şekilde verebilirsin.



ŞİFRELERİN SAĞLAM MI?

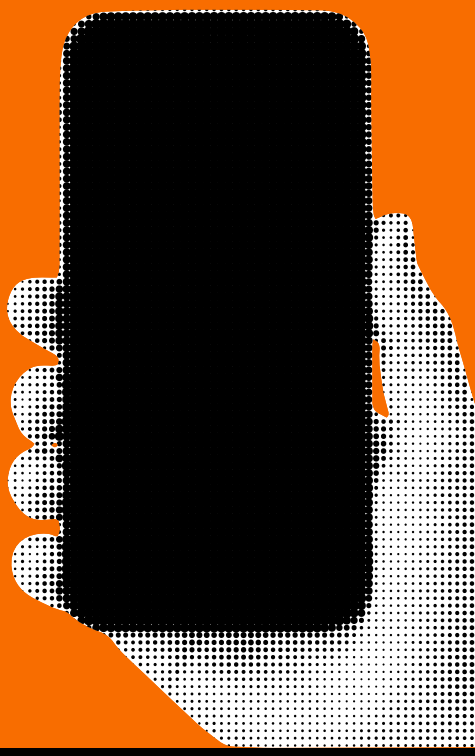
Şifrelerini belirli aralıklarla değiştirmeli ve “12345”, “qwerty” ya da “qwerty123” gibi çok kullanılan ve en kolay tahmin edilebilen şifrelerden birini kullanmamalısın. Bu gibi şifreleri kırmak bir saniyeden daha kısa sürdüğü için dijitaldeki güvenliğin için büyük bir tehdit oluşturur.

Şifrelerini de belirli aralıklarla değiştirmeyi unutma. Öte yandan şifrelerin kişisel veridir, sevdiklerin bile olsa bir başkası ile paylaşmamalısın.

GÜVENLİK SORUNUN CEVABINI SADECE SEN Mİ BİLİYORSUN?

Kayıt olurken dijital platformlar, şifreni unutman halinde yardımcı olması için bir güvenlik sorusu ve cevabı belirlemeni ister. Bu güvenlik sorusunun cevabını sadece senin bildiğinden emin ol. Bu konuda çevrendekilerle konuşurken dikkat et, farkında olmadan bu sorunun cevabını paylaşıyor olabilirsin.

Aynı zamanda dijital platformlarda, özellikle de güvenlik sorun çocukluğuna dair ise (ilk evcil hayvanın, ilkokulunun adı, en sevdiğin ilkokul öğretmenin vb.), geçmiş anıların paylaşıldığı #tbt (Kullanıcıların geçmişe dair anılarını #ThrowBackThursday etiketi ile paylaştığı akım) gibi akımlarda neler paylaştığına dikkat et.



ÇOK PLATFORM, TEK ŞİFRE?

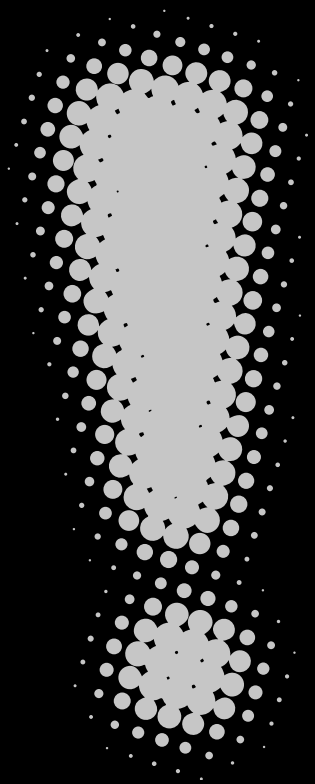
Üyesi olduğun bütün dijital platformlarda aynı şifreyi kullanmak güvenliğini tehlikeye atacaktır. Hatta bütün platformlarda aynı kullanıcı adı ve şifre kombinasyonunu kullanmak daha da tehlikeli olabilir.

Bir dijital platformun veri sızıntısı yaşaması durumunda eğer sızan veri kullanıcı adı ve şifrelerse bu bilgiyi ele geçiren kişi veya kişiler bu kombinasyonu başka platformlarda da deneyebilir, başka platformlardaki profillerine de erişebilir.

GÜVENLİK AYARLARINI YAPTIN MI?

Dijital platformlarda daha en başta güvenlik ve gizlilik kısımlarına girip gerekli gördüğün ayarları yapmalısın. Üye olurken kullandığın e-posta adresi ya da telefon numarasının platform içinde kimler tarafından görülebileceğini seçmek, içeriklerinin kimlere gösterileceğine karar vermek, yorumlarda hangi kelimelerin filtreleneceğini belirlemek, takipçilerinin hangi davranışlarını sınırlandırabileceğine dair ayarları yapmak bunlardan sadece birkaçı.

Örneğin Instagram'da istenmeyen yorum ve mesajları geçici olarak sınırlayabilmeni sağlayan sınırlı etkileşimler özelliğini kullanmak daha güvende hissetmeni sağlayabilir.



İKİ FAKTÖRLÜ DOĞRULAMAYI AÇTIN MI?

Çoğu dijital platformda iki faktörlü doğrulama özelliği bulunmakta. Bu özellik sayesinde hesabına farklı bir cihazdan girmek istediğinde sana bir kod ya da tercih ettiğin doğrulama metodu ile bir bildirim gönderilir. Bu doğrulamayı yapmadan hesabına giriş yapmana izin verilmez. Bu sayede cihaz ya da tarayıcı değiştirdiğinde hesabına güvenli bir şekilde giriş yapabilirsin.

ÜÇÜNCÜ PARTİ UYGULAMALARA İZİN VERDİN Mİ?

Daha önce üyesi olmadığın bir dijital platformda bazen yeni bir profil oluşturmak yerine Google, Facebook ya da halihazırda üye olduğun benzer bir platform ile giriş yapmak sana çok daha kolay ya da hızlı gelebilir. Fakat bu durumda yeni üye olacağın platform, mevcutta üyesi olduğun platformdaki verilerine erişebiliyor ve bu da güvenlik açığına yol açabiliyor. Bu erişimleri güvenlik ayarlarından geriye dönük kaldırabiliyorsun.

Örneğin Google hesabının güvenlik kısmında “Üçüncü taraf uygulamaları ve hizmetleri” bölümünde hangi uygulamalara erişim verdiğini görüntüleyip, hatırlamadığın ya da bilmediğin uygulamaları kaldırman sağlıklı olacaktır.

ŞİKAYET MEKANİZMALARINI KULLANIYOR MUSUN?

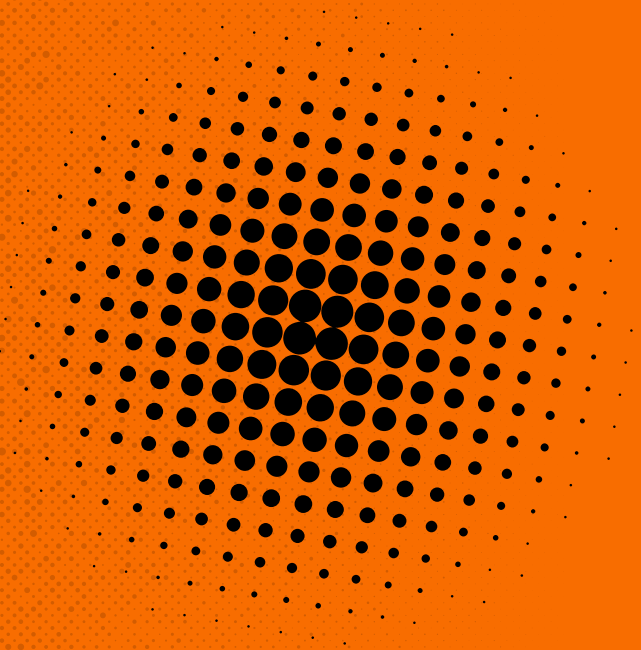
Dijital şiddete maruz kaldığında, olayın gerçekleştiği dijital platformun şikayet mekanizmasını kullanmalısın. Bunu yaparak dijital platformların hem kendin hem de bütün kullanıcılar için daha güvenli bir hale gelmesini sağlayabilirsin.

Şikayet mekanizmalarında dikkat etmen gereken nokta, şikayetinin doğru bir şekilde değerlendirilebilmesi için ilgili başlık altında yapmış olman. Aynı zamanda bir profili, bir içeriği, bir videonun kapak görselini ya da bir videoyu ayrı ayrı şikayet edebildiğini / raporlayabildiğini de unutma. Şikayet başlıkları platformdan platforma değişebileceği gibi zaman içinde de güncellenebilir. Dolayısıyla dönem dönem şikayet menülerine göz gezdirmekte fayda var.

ORTAK KULLANIM ALANLARINDA GÜVENLİĞİNE DİKKAT EDİYOR MUSUN?

Ortak kullanım alanlarında ya da tanımadığın kişilerin de erişimi olan internet bağlantıları yerine kendi internet bağlantını kullanmak daha sağlıklı olur. Hatta bilgisayar için internet bağlantısına ihtiyacın olunca telefonunu modem olarak kullanmayı tercih edebilirsin.

Ayrıca ortak kullanım alanlarına ait bir bilgisayarları kullandığın zaman giriş yaptığın bütün platformlardan çıkış yapmayı, tarayıcı geçmişini temizlemeyi de unutma.

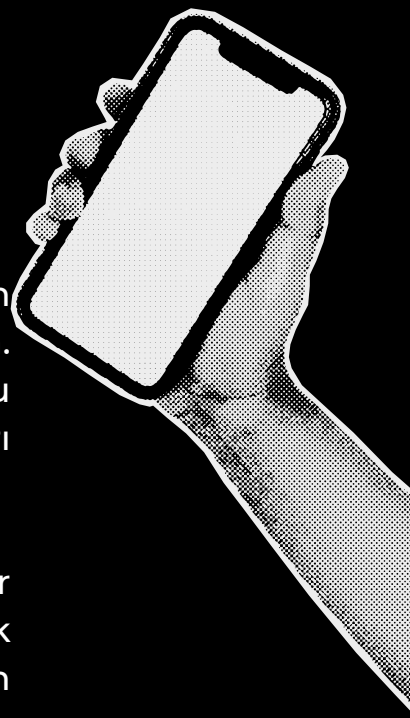


KONUM BİLGİSİ PAYLAŞIYOR MUSUN?

Dijital şiddete maruz kalmaya açık olduğunu düşündüğün zamanlarda (ısrarlı takip eden bir partner vb.) anlık konum bilgisi paylaşmamanda fayda var.

Herhangi bir mekandan yer bildirimi yapmak, henüz mekandan ayrılmamışken yüklediğin fotoğrafa konum bilgisi eklemek gibi şeylerden kaçınarak kendini güvende tutmalısın.

CİHAZINDA BİLMEDİĞİN BİR UYGULAMA VAR MI?



Telefon, bilgisayar ya da tabletini düzenli olarak senin kurmadığın bir uygulamanın olup olmadığını kontrol etmelisin. Eğer tanımadığın bir uygulama ile karşılaşırsan kaldırmalısın. Bu uygulamalar seni takip etmek için cihazlarına başkaları tarafından kurulmuş olabilir.

Bu kontrol en çok tuş vuruşu kaydı (bir bilgisayarda yapılan her tuş vuruşu girişinin takip ve kayıt edilmesi) ve "keylogger" olarak geçen klavyede bir harfe dokunulduğunda casus yazılımın dinlemesi ve klavye harflerini kaydetmesini sağlayan sistemlerin tespit edilmesi için önemlidir. Bu durumla en çok hediye gelen ve teknik servisten dönen cihazlarda karşılaşılıyor.

Bazı uygulamalar sistem uygulaması olabilir, dolayısıyla bilmediğin /tanımadığın bir uygulama ile karşılaşınca silmeden önce internette aratmakta fayda var.

TELEFONUNU SERVİSE VERMEN GEREKTİĞİNDE...

Android işletim sistemi kullanan bazı telefonların "Ayarlar" kısmından "Pil ve Cihaz Bakımı"nın altında ya da "Hızlı Servisler"in altında "Bakım modu" özelliği mevcut.

Bakım modunu aktif hale getirirsen telefonda sadece temel bazı uygulamalar görünür olur ve şahsi bilgilerinin hiçbirine erişilemez. Bakım modundan çıkmak için de telefonunun şifresine ihtiyaç vardır. Bu özellik sayesinde telefonun servise gittiğinde teknik ekip hiçbir özel bilgini görüntüleyemez.

iPhone veya iPad'ini servise götürmeden önce ise cihazını yedekle, Apple Cash'i kapat, Apple Cüzdan'dan kartları ve ulaşım kartlarını kaldır ve Bul'u kapat.

CİHAZINI DEĞİŞTİRİRKEN HER YERDEN ÇIKIŞ YAPTIN MI?

Telefon, tablet ya da bilgisayar değiştireceğin zaman, telefonu fabrika ayarlarına döndürmeden önce bütün uygulamalardaki hesaplarından çıkış yaptığından emin ol. Başka bir cihazda kullandığın dijital platformların güvenlik ayarları kısmından hesabının aktif olarak hangi cihazlarda tanımlandığını kontrol edebilirsin.

Kullandığın uygulamaların güvenlik ayarlarının her bölümünü mobilden görüntüleyemeyebilirsin. En sağlıklısı bilgisayarlarda tarayıcıdan ilgili platforma giriş yaparak güvenlik ayarlarını kontrol etmektir.



OLTAYA GELMEDİĞİNDEN EMİN MİSİN?

Sana gönderilen e-postalar her zaman iyi niyetli olmayabilir. Bazen bir e-postada bulunan bir bağlantıya tıkladığında ya da bir eki açtığında bilgisayarına verilerini toplaması veya hareketlerini takip etmesi için gönderilen kötücül bir yazılımı aktif hale getirmiş olabilirsin. Bu kötücül yazılımlar bazen abonesi olmadığın bir operatörden gelen ve pdf formatında gibi görünen bir faturada, bazen de arkadaşının tatilde çektiğini iddia ettiği fotoğrafları görüntülemen için paylaşılan bir bağlantıda gizli olabilir.

Oltalama (phishing) olarak da geçen bu yönteme dair ne kadar bilgili olduğunu test etmek için: **https://phishingquiz.withgoogle.com**

Başkaları için de yapabileceklerin var!

- Başkalarının maruz kaldığı dijital şiddeti ilgili sosyal medya platformuna şikayet edebilirsin.

- Tanıdığın ya da tanımadığın, dijital şiddete maruz kalan birine yalnız olmadığını göstermek için bir dayanışma mesajı gönderebilirsin.

- Fail, bir tanıdığın olabilir. Böyle bir durumda şiddete maruz kalan kişiye dair kafanda bahaneler üretirken kendini yakalarsan düşüncelerini sorgula ve şiddetin hiçbir bahanesi olmadığını unutma.

- Nefret söylemi içeren içerikleri, cinsiyetçi söylemleri takdir etmemeli ve yeniden paylaşarak dolaşıma sokmamalısın.

- Tüm paylaşımlarında etiketlediğin kişilerden izin almanda fayda var. Bir fotoğraf etiketlemesinin kimler için nasıl bir güvenlik tehlikesi oluşturacağını bilemezsin!

Ve tabii ki her şeyden önce bu rehberi paylaşmakla başlayabilirsin...

Referanslar:

[1]OHCHR (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.

[2]UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[3]UNFPA (2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[4] UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[5] Sensity AI. (2019). The state of deepfakes: A deepfake landscape and threat report.

[6] IPSOS (2024). International Women's Day 2024: Global Attitudes Towards Women's Leadership.

[7] Center for Countering Digital Hate (2022) The Incelosphere: Exposing pathways into incel communities and the harms they pose to women and children.

[8] UNGA 79: Intensıfıcatıon of Efforts to Eliminate All Forms of Violence Against Women and Girls: Technology Facilitated Violence Against Women and Girls Report of the UN Secretary General (2024)

[9] UN Women (2023). The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia.

[10] TBİD (2021). Türkiye'de Dijital Şiddet Araştırması.

[11] Bu bölüm, Dunn (2020) ve UNFPA (2021) raporlarından derlenmiştir.
Dunn, S. (2020). Supporting a Safer Internet Paper No. 1: Technology-Facilitated Gender-Based Violence: An Overview. Centre for International Governance Innovation (CIGI).
UNFPA (2021). Technology-Facilitated Gender-Based Violence: Making All Spaces Safe.

[12] UNESCO (2021). The chilling: global trends in online violence against women journalists

[13] Inter-Parliamentary Union (2016). Sexism, harassment and violence against women parliamentarians

[14] Un Women (2023). Türkiye'de Siyasette Kadınlara Yönelik Şiddet.

[15] Plan International (2020). Free to Be Online? Girls' and young women's experiences of online harassment

[16]16 UN Women (2023). The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia.

[17]TBİD (2021). Türkiye'de Dijital Şiddet Araştırması.

[18] EWL (2024). Report on Cyber Violence Against Women.

Kavram Kartları Referanslar:

[19] UNFPA(2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[20] UN Women. How to address online sexual harassment during COVID-19.

[21] https://tfgbv.humane-intelligence.org/abuse-type/cyberstalking.

[22] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[23] European Parlement(2018). Cyber violence and hate speech online against women.

[24] Pen America. Defining "Online Abuse": A Glossary of Terms.

[25] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[26] WMC. Online Abuse 101.

[27] WomensLaw (2024). Abuse Using Technology.

[28] https://womensmediacenter.com/speech-project/online-abuse-101

[29] https://tfgbv.humane-intelligence.org/abuse-type/voyeuristic-recording/

[30]https://tfgbv.humane-intelligence.org/abuse-type/doxxing.

[31] https://womensmediacenter.com/speech-project/online-abuse-101.

[32] https://techterms.com/definition/flaming.

[33] UNFPA (2024). Digital Duality: How the Internet Empowers and Endangers Women

[34] Foreign, Commonwealth & Development Office (2023). Technology-facilitated gender-based violence: preliminary landscape analysis.

[35] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[36] UNFPA(2021). Technology-facilitated Gender-based Violence: Making All Spaces Safe.

[37] Pen America. Defining "Online Abuse": A Glossary of Terms.

[38] https://tfgbv.humane-intelligence.org/abuse-type/iot-abuse.

[39] WMC. Online Abuse 101.

[40] https://tfgbv.humane-intelligence.org/abuse-type/online-impersonation.

[41] European Women's Lobby (2024). Report on Cyber Violence Against Women.

[42] European Womens' Lobby #KadınınİnternetiKadınınHakkı Rehberi

[43] https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.359

[44] https://womenlobby.org/new-publication-report-on-cyber-violence-against-women/

[45] Suzie Dunn, "Technology-facilitated gender-based violence: an overview", https://apo.org.au/node/309987

[46] https://en.wikipedia.org/wiki/Shadow_banning

[47] https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

[48] https://womenlobby.org/new-publication-report-on-cyber-violence-against-women/

[49] https://www.unwomen.org/en/articles/explainer/what-is-the-manosphere-and-why-should-we-care

[50] https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

[51] https://apo.org.au/node/309987

DİJİTAL ŞİDDETE NOKTAYI KOY!

turkiye.unfpa.org
infoturkiye@unfpa.org

turkiye.unwomen.org
infoturkiye@unwomen.org

@unwomenturkiye
@unfpaturkiye