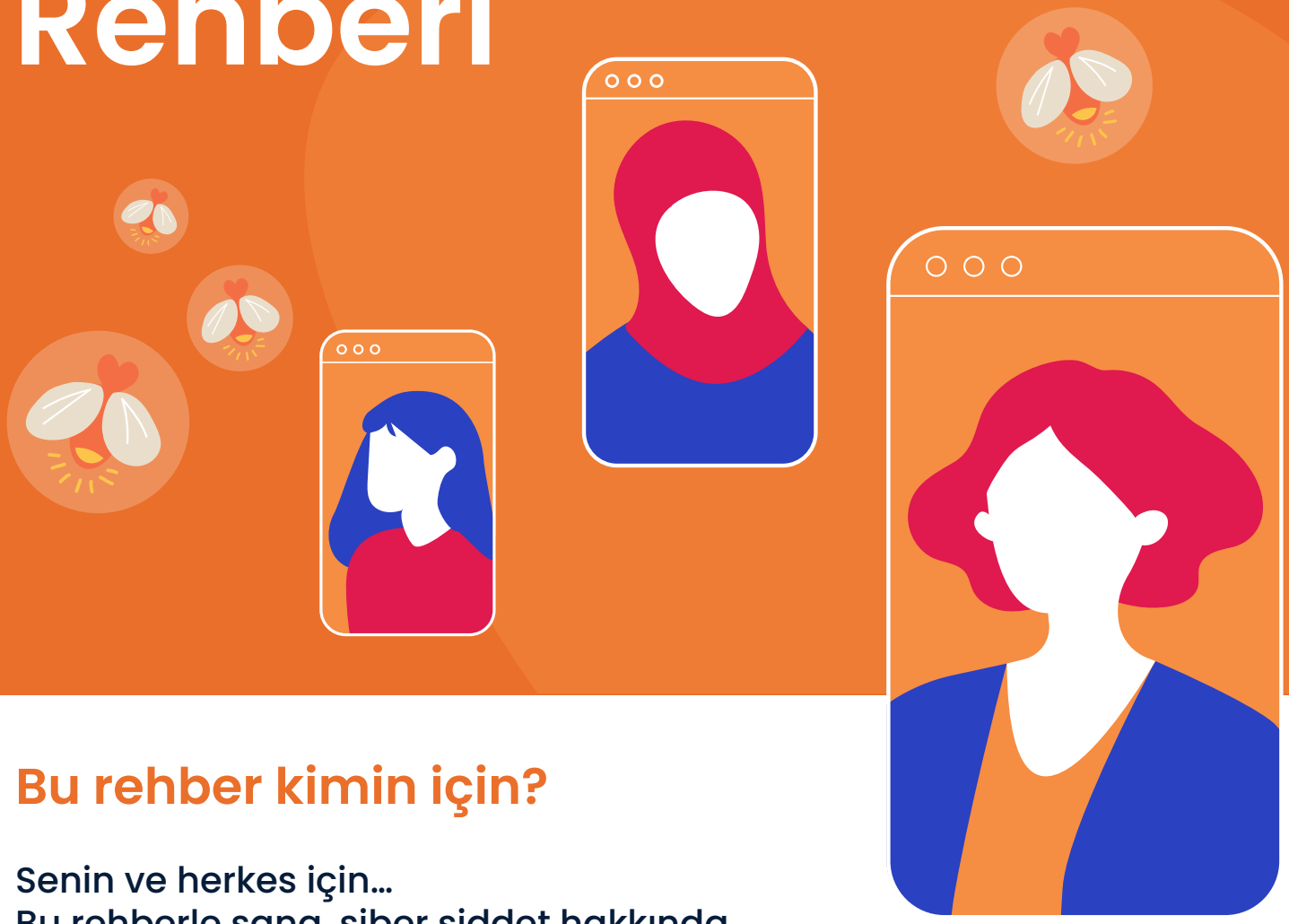
İsveç Sverige

UN WOMEN

Toplumsal Cinsiyete Dayalı Siber Şiddet Rehberi



Bu rehber kimin için?

Senin ve herkes için...
Bu rehberle sana, siber şiddet hakkında bilgiler vermek ve dijital alanda kontrolü ele alman için yol göstermek istiyoruz.

@UNWomenTurkey

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].

Kadınlara yönelik şiddet, toplumsal cinsiyete dayalı diğer şiddet türlerini de içinde barındırıyor. Bunlar arasında, cep telefonları ve akıllı telefonlar, internet, sosyal medya platformları ve e-posta gibi bilişim ve iletişim teknolojileri kullanılarak kadınlara, kadın olmalarından ötürü uygulanan siber şiddet de bulunuyor.

Günümüzde siber şiddetin henüz ortak bir tanımı bulunmuyor ve yeterli veriye sahip değiliz. Fakat bu alandaki terminoloji her gün daha da zenginleşiyor.

Olayların dijital ortamlarda yaşanması şiddetin derecesini azaltmıyor!

Toplumsal cinsiyete dayalı şiddetin her türlüsü gibi siber şiddet de bir insan hakları ihlalidir ve eşitsizliklerin bir sonucudur!

Dünya genelinde pandemi dönemi ile birlikte eşitsizlikler derinleşmekte, toplumsal cinsiyete dayalı şiddetin bir biçimi olan siber şiddet de artmaktadır.[2]

Siber şiddete kim maruz bırakılıyor?

Herkes!

Ancak siber şiddet, toplumsal cinsiyete dayalı şiddet ile aynı yapısal eşitsizliklerden ve ayrımcılıktan kaynaklandığı için kadınların ve kız çocuklarının maruz bırakıldığı şiddet daha farklı ve fazladır.

Avrupa Birliğinde yaşayan kadınların %23'ü, hayatlarında en az bir kez siber tacize veya istismara maruz bırakıldığını belirtiyor. Her 10 kadından biri ise 15 yaşından itibaren en az bir şiddet türüne maruz bırakıldığını söylüyor[3]**.**

Kadınlar; eğitimleri, yaşları, meslekleri, pozisyonları, cinsel yönelimleri, ırk ve etnik kökenleri, ilişki durumları nedeniyle çeşitli siber şiddet içeren davranışlara, çoklu ayrımcılık biçimlerine maruz bırakılma riskiyle karşı karşıya.

Dijital ortamlarda daha göz önünde olan kadınlar, siber şiddete daha fazla maruz bırakılıyor[4]: Siyasetçi, gazeteci, sanatçı, yazar, akademisyen ve/veya aktivist olan kadınlar dönem dönem siber şiddet faillerinin açık hedefi haline gelebiliyor.

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

15-24 yaş arasında gençlerin yüzde 94'ünün çevrim içi[5] olduğunu biliyoruz.

UNICEF'in, dünya genelinde bir milyon gençle yaptığı bir ankete göre, gençlerin yüzde 70'ten fazlası siber şiddete maruz bırakılıyor[6].

Türkiye'de de siber şiddete en çok 25-40 yaş aralığındakiler maruz bırakılıyor[7].

Siber şiddeti uygulayan kim(ler)?

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

Siber şiddet bizim hatamız değildir! Şiddet suçtur ve işleyen fail(ler) için cezası 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...

Siber şiddet nerede ve nasıl gerçekleşir?

Siber 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.

İstersen örneklerle biraz bu konuyu pekiştirelim...

Siber şiddetin farklı türleri var:

Bunlardan ilki **siber takip.** Diğer bilinen adıyla "Stalklama" bazen hiç masum olmayabilir!

Siber takip; e-posta, çevrim içi mesajlar veya internet yoluyla izlenmedir.

Hiç haberimiz olmadan casus yazılım veya klavye kaydediciler ile hareketlerimiz izlenebilir.

En fazla karşılaşılan diğer bir tür de de **siber taciz.** Birkaç örnek vermek gerekirse:

- İstenmeyen cinsel içerikli e-postalar, mesajlar
- Dijital platformlardan paylaşılan uygunsuz veya saldırgan mesajlar, fiziksel ve/veya cinsel şiddet tehditleri

Özellikle çocukluk ve gençlik dönemlerinde yaşanan diğer bir tür de **siber zorbalıktır.**

Siber zorbalık dijital teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Bu tür zorbalıklar sosyal medyada, mesajlaşma platformlarında, oyun platformlarında ve cep telefonlarında görülebilir. Hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranıştır[8].

Maruz kalan üzerinde en ağır etkileri yaratabilecek diğer bir tür de **görsel-odaklı cinsel tacizdir.**

Görsel-odaklı cinsel taciz; görüntüde yer alan kişinin rızası olmaksızın cinsel içerikli fotoğraflarının veya videolarının çevrim içi olarak dağıtılmasıdır.

Fail, genellikle önceki bir ilişki esnasında görüntü veya video elde eden eski bir eş ya da partnerdir. İlişkiyi bitirmemek ya da bazı taleplerde bulunmak için görüntüleri tehdit amaçlı kullanır. Failler, mutlaka eski eş ya da partner olmayabilir, hiç tanımadığımız biri de bilgisayarımıza/hesaplarımıza erişerek görüntülerimizi tehdit amaçlı kullanabilir.

İznimiz olmadan özel verilerimize erişilmesi de (kişisel hesaplarımızın ele geçirilmesi, şifrelerin çalınması vb.) **gizlilik ihlalidir.**

Örneklerini sıralayalım:

- Fotoğraf ve videolarımıza iznimiz dışında erişme ya da bunları alma, kullanma, manipüle etme, dağıtma,
- Bilgimiz dışında veya onayımız olmadan (cinsel içerikli) görüntüler, ses klipleri, video klipler de dahil olmak üzere özel bilgi ve içeriği kaydetme, paylaşma, yayma,
- Catfishing olarak da bilinen bir yöntem ile birinin bizim kimliğimizi kullanarak, bizim adımıza profil oluşturması,
- Doxing olarak bilinen diğer bir yöntemle de iznimiz ve rızamız olmadan kişisel bilgilerimizin araştırılması, toplanması ve taciz amacıyla yayınlanması,
- Bizimle temas kurmak ya da bizi utandırmak için, ailelerimize, arkadaşlarımıza, iş arkadaşlarımıza ulaşma ve onları taciz etme.

Siber şiddetin etkileri neler?

Siber şiddete maruz bırakıldığımızda "öfke, şaşkınlık çaresizlik, güçsüzlük, kendi güvenliğimiz konusunda endişe etme, korku ve üzüntü" hissedebilir "aile ve arkadaşlarımızın duymasından" endişe edebiliriz.

Yaşadığımız şiddeti önemsizleştirebilir, kendimizi suçlayabilir ve olayları değiştirmek için yapabilecek hiçbir şey olmadığı inancına kapılabiliriz. Hatta sosyal medya hesaplarımızı kapatabilir veya internet kullanmayı tümüyle bırakabiliriz.

Bir sosyal medya hesabının kapatılması küçük bir şey gibi görünebilir. Ancak, bu özellikle kadınların ve kız çocuklarının dijital alanlardan çekilmesi anlamına geliyor. Kamusal, özel ve dijital alanlarda kendini güvenli ve özgür hissetmek ve ifade edebilmek hepimizin hakkıdır.

Yaşadığımız kafa karışıklığı, ne yapacağımızı bilememe hali çok normal.

Kadınlar genellikle siber şiddet sonucu korku, endişe ve depresyona maruz kalmaktadır; ki bu da çevrim içi alanlardan çekilmelerine yol açmaktadır. Şiddete maruz bırakılanların sosyal hayatları ve iş yaşamları sıklıkla etkilenmekte, hareketlilikleri sınırlanmaktadır.

Neler yaparak kendini güvende tutabilirsin?

Çevrim içi hedef olmak, utanmana, güvensiz hissetmene, kendini suçlamana ve işlerin tamamen kontrolden çıktığını hissetmene neden olabilir. Bazen hiçbir şey de yapmak 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!

Her gün kendine zaman ayırabilir, çevrim içi dünya ile belirli bir süre için arana mesafe koyabilirsin. Kendi kendine ya da arkadaşlarınla sevdiğin bir şeyler yapabilirsin.

Kanıt topla!

Yaşadığın siber şiddeti / olayları belgele. Şikayet için yasal yollara başvurduğun zaman bu belgelere ihtiyacın olacak. Ayrıca bu belgeler durumunu görmene ve güvenlik planlaması yapmanda sana yardımcı olabilir.

Ekran görüntüsü almayı unutma! Hatta aldığın ekran görüntülerinin çıktılarını da al!

Şikayetçi olmaya karar verirsen...

Haklarının ne olduğu konusunda bilgi sahibi olman gerek.

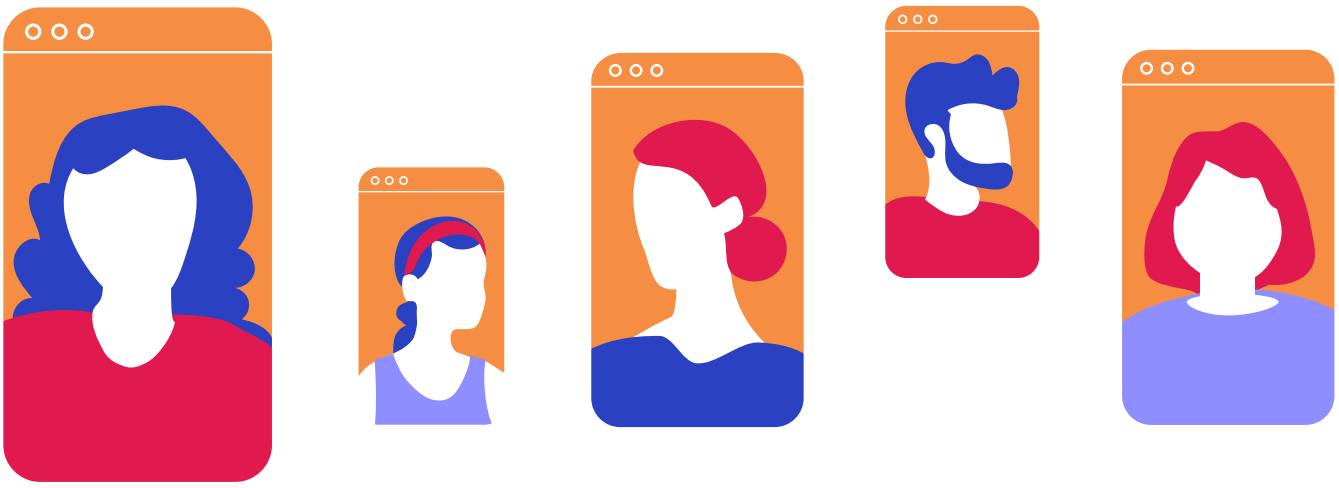
Yasal süreçleri öğrenmek için konu ile ilgili çalışan avukatlar ile Baroların Kadın Danışma Merkezleri-Komisyonları ile görüşebilirsin.

Polis-Jandarma birimlerine veya Savcılığa suç duyurusunda bulunabilirsin. Öncesinde ilgili tüm kanıtları toplamayı 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. Gizliliğini koruyacaklarından emin ol!

Unutma, kişisel verilerinin ve özel hayatının gizliliğinin korunmasını istemek temel haklarındandır.



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

Uluslararası Sözleşmeler:

- **Kadınlara Karşı Her Türlü Ayrımcılığın Önlenmesi Sözleşmesi (CEDAW)**
- **Kadına Yönelik Şiddet ve Aile İçi Şiddetin Önlenmesi ve Bunlarla Mücadeleye Dair Avrupa Konseyi Sözleşmesi (İstanbul Sözleşmesi)**
- **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**

Başvurabileceğin kurumlar:

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

Arayabileceğin Acil Telefon Hatları:

- 155 Polis
- 156 Jandarma
- 112 Acil Çağrı Merkezi
- Alo 183 Aile, Kadın, Çocuk ve Engelli Sosyal Hizmet Danışma Hattı
- 0212 656 96 96 / 0549 656 96 96 Aile İçi Şiddet Acil Yardım Hattı
- Türkçe dışında bir dil konuşuyorsan 157 Yabancılar İletişim Merkezi

Çevrim içi Başvurabileceğin Yerler:

https://www.turkiye.gov.tr/btk-internet-ihbar-basvurusu

https://onlineislemler.egm.gov.tr/Sayfalar/Ihbar.aspx

155@iem.gov.tr

Dijital güvenliğin için yapabileceklerin...

Dijital Dünyada Kontrolü Elimize Alıyoruz!

Şifrelerin sağlam mı?

Şifrelerini belirli aralıklarla değiştirmeli ve "12345" gibi dünyada en çok kullanılan[9] ve en kolay tahmin edilebilen şifrelerden birini kullanmamalısın. Dijital platformların güvenlik sorularına verdiğin cevaplara dair de paylaşımlarda bulunmamalısın.

Bütün platformlarda aynı şifreyi kullanmak da güvenlik açığına yol açacaktır. Öte yandan şifreleriniz kişisel veridir, sevdikleriniz bile olsa bir başkası ile paylaşmamanız gerekir.

Şikayet mekanizmalarını kullanıyor musunuz?

Siber şiddete maruz bırakıldığında, olayın gerçekleştiği dijital platformun şikayet mekanizmasını kullanmalısın. Bunu yaparak dijital platformların hem senin 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 yapılmış olması gerektiği. Örneğin, Instagram'da bir kişi sen ya da bir tanıdığın gibi davranıp senin fotoğraflarınla hesap açtıysa, hesabı şikayet ederken "Şikayet et" butonuna basıp ardından "Spam" seçmek yerine, önce "Uygunsuz"u, ardından "Hesabı Şikayet Et"i , ardından "Bir başkasını taklit ediyor"u seçip "Beni/Tanıdığım birisini/Bir ünlü veya tanınmış kişiyi" seçeneklerinden birini işaretlemelisin..

Güvenlik ayarlarını yaptın mı?

Dijital platformlara üye olurken verdiğin e-posta adresi ya da telefon numarasının platform içinde kimler tarafından görülebileceğini seçebiliyorsun. Aynı zamanda üye olduğun platformun içinde, platformun arama motoru vasıtasıyla bulunup bulunmamak da seçebileceğin bir özellik. Hatta bazı platformlarda bulunan "yüz tanıma" gibi özellikleri de kapatabilirsin.

Tek yapman gereken üye olduğun platformun güvenlik ayarlarını gözden geçirmek. Bir platforma üye olduğunuzda güvenlik ayarlarını, herhangi bir paylaşımda bulunmadan önce yapmanda fayda var.

İki faktörlü doğrulamayı açtın mı?

Çoğu dijital platformda iki faktörlü doğrulama özelliği bulunmaktadır.
Bu özelliği kullandığında hesabına farklı bir bilgisayardan girmek istediğinde sana bir kod gönderiliyor. Bu da cihaz ya da tarayıcı değiştirdiğinde güvenli bir şekilde hesabına giriş yapmanı sağlıyor.

Ortak kullanım alanlarında güvenliğine dikkat ediyor musun?

Ortak kullanım alanlarında ya da gittiğin mekanlarda mümkünse tanımadığın kişilerin de erişimi olan internet bağlantıları yerine kendi internet bağlantını kullan. Hatta bilgisayar için internet bağlantısına ihtiyacın olunca telefonunun modem olarak kullanılabilme özelliğini (Hotspot) tercih edebilirsin.

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

Üçüncü partilere izin verdin mi?

Dijital platformlarda uygulamalara girerken ya da uygulamaların içindeki bazı özellikleri kullanmak için, başka bir platformdaki üyeliğinle erişim sağladığında da güvenlik açığına yol açabilirsin. Örneğin, bir platforma girerken oraya özgü bir kullanıcı adı ya da şifre oluşturmak yerine Google, Facebook ya da Twitter hesabınla giriş yapmak gibi. Kullandığın platformun güvenlik ayarlarının içinden izin verdiğin üçüncü parti uygulamalara göz atıp gereksiz olanları kaldırmak faydalı olacaktır.

Konum bilgisi paylaşıyor musun?

Siber şiddete açık olduğunu düşündüğün zamanlarda konum bilgisi paylaşmamanda fayda var.

Cihazında bilmediğin bir uygulama var mı?

Telefon ya da bilgisayarını düzenli olarak kontrol edip senin kurmadığın uygulamaları kaldırmalısın. Bu uygulamalar cihazlarına, seni takip için başkaları tarafından kurulmuş olabilir.

Oltaya gelmediğinden emin misin?

Sana gönderilen e-postalar her zaman iyi niyetli olmayabilir. Adını MALicious SoftWARE'den (kötü amaçlı yazılım) alan Malware, sana gelen bir e-postada bulunan bir bağlantıyı açtığında ya da bir eke tıkladığında, eki indirip açmak istediğinde bilgisayarına tüm verilerini toplaması için bir virüs gönderen yazılımlardır.

Bir e-postanın Malware barındırıp barındırmadığını anlamak için öncelikle gönderenin e-posta adresini ve ekinin dosya formatını kontrol etmekte fayda var.

Oltaya gelip gelmeme konusunda ne kadar bilgili olduğunuzu test etmek için: https://phishingquiz.withgoogle.com

Başkaları için de yapabileceklerin var!

- Başkalarının maruz bırakıldığı siber şiddeti ilgili sosyal medya platformuna şikayet edebilirsin.
- Tanıdığın ya da tanımadığın, siber şiddete maruz bırakılan birine yalnız olmadığını göstermek için bir dayanışma mesajı gönderebilirsin.
- Fail, bir tanıdığın olabilir. Böyle bir durumda şiddete maruz bırakılan 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!

Bu rehberi arkadaşlarına göndermek ile başlayabilirsin...

---

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. Available at https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx

2 UN Women (2020). Online and ICT facilitated violence against women and girls during COVID-19

3 European Union Agency for Fundamental Rights (2014). Violence against women: an EU-wide survey, p. 104.

4 IGF. (2015). Internet Governance Forum-Best Practice Forum on Online Abuse and Gender-Based Violence Against Women

5 ITU (2020) BM Uluslararası Telekomünikasyon Birliği verileri

6 UNICEF (2019). Safer Internet Day UNICEF calls for concerted action https://www.unicef.org/press-releases/safer-internet-day-unicef-calls-concerted-action-prevent-bullying-and-harassment

7 Microsoft (2019). Dijital Nezaket Araştırması

8 UNICEF (2019). Siber zorbalık: Nedir ve nasıl önlenir https://www.unicef.org/turkey/siber-zorbal%C4%B1k-nedir-ve-nas%C4%B1l-%C3%B6nlenir

9 Teampassword (2019). Top 50 Worst Passwords of 2019 https://www.teampassword.com/blog/top-50-worst-passwords-of-2019

Kaynaklar:
Temur, N. (2019). Toplumsal Cinsiyete Dayalı Siber Şiddet -Kadın Örgütleri için Rehber

İlkiz, P., Tekin, A. ve Temur, N. (2019). Avrupa Kadın Lobisi - #KadınınİnternetiKadınınHakkı / #HerNetHerRights Türkiye Kampanyası Eğitim Materyalleri

Yazarlar: Nurcihan Temur, Pınar İlkiz

Bu yayın, İsveç'in İsveç Uluslararası Kalkınma İşbirliği Ajansı (SIDA) aracılığıyla verdiği destek ile hayata geçirilmiştir. Yayında dile getirilen görüşler yazar(lar)a ait olup, UN Women, Birleşmiş Milletler, ilgili organizasyonları ya da İsveç'in görüşlerini yansıtmak zorunda değildir.

İsveç Sverige

UN WOMEN