Diyarbakır gibi büyük, hareketli ve farklı sosyal çevrelerin iç içe geçtiği bir şehirde internet üzerinden yapılan kişisel hizmet aramaları, son yıllarda ciddi biçimde dijital ortama kaydı. İnsanlar artık telefon rehberinden, tanıdık çevresinden ya da fiziksel ilanlardan çok arama motorları, sosyal medya hesapları, mesajlaşma uygulamaları ve ilan siteleri üzerinden bilgi toplamaya çalışıyor. Bu durum, sadece erişimi kolaylaştırmadı; aynı zamanda dolandırıcılık riskini de artırdı.

“diyarbakır escort bayan”, “Escort bayan diyarbakır” ya da “Bayan escort diyarbakır” gibi aramalar yapan kişilerin karşılaştığı sonuçların önemli bir kısmı doğrulanması zor içeriklerden oluşur. Aynı fotoğrafı kullanan onlarca farklı profil, birbirine benzeyen metinler, sahte yorumlar, kopyalanmış telefon numaraları ve ön ödeme isteyen hesaplar, bu alanda sık görülen riskler arasında yer alır. Üstelik dolandırıcılık her zaman kaba saba bir yöntemle yapılmaz. Bazı kişiler oldukça profesyonel görünür, düzgün Türkçe kullanır, güven verici konuşur ve karşı tarafı adım adım ikna eder.

Bu yazı, herhangi bir hizmeti teşvik etmek için değil, internet üzerinde riskli aramalar yapan kişilerin dolandırıcılık, şantaj, veri hırsızlığı ve kişisel güvenlik sorunlarına karşı daha dikkatli davranabilmesi için hazırlanmıştır. Konu hassas olduğu için meseleye ahlaki yargılardan çok pratik güvenlik açısından bakmak gerekir. Çünkü dijital dolandırıcılık, kişinin niyetinden bağımsız olarak maddi kayba, itibar zedelenmesine ve hukuki sorunlara yol açabilir.

Arama sonuçlarının güvenilir görünmesi güvenli olduğu anlamına gelmez

Google’da üst sıralarda çıkan bir sayfanın, otomatik olarak güvenilir olduğu düşünülür. Oysa arama motorlarında görünürlük ile gerçek güvenilirlik aynı şey değildir. Bir site teknik olarak iyi hazırlanmış olabilir, anahtar kelimeleri doğru kullanmış olabilir, hatta profesyonel görseller ve düzenli içeriklerle desteklenmiş olabilir. Bu, sitedeki kişilerin gerçek olduğu ya da verilen bilgilerin doğrulandığı anlamına gelmez.

Diyarbakır özelinde yapılan aramalarda, aynı ilan metninin farklı ilçeler için kopyalandığı sık görülür. Bağlar, Kayapınar, Yenişehir veya Sur gibi merkez ilçelerin adı yalnızca metne yerleştirilmiş olabilir. Profilde anlatılan kişiyle kullanılan fotoğrafın ilgisi olmayabilir. Bazı sayfalarda ise “doğrulanmış profil”, “güvenilir ilan”, “VIP” gibi ifadeler yer alır; fakat bu ibarelerin arkasında bağımsız bir denetim yoktur. Site sahibi kendisi bu etiketi koymuş olabilir.

Bir başka sorun da telefon numaralarının sürekli değişmesidir. Dolandırıcılar, kısa süreli kullanılan hatlar veya internet tabanlı mesajlaşma hesapları üzerinden iletişim kurar. Bir numara birkaç gün aktif kalır, ardından kapatılır ya da başka bir isimle yeniden kullanılır. Bu nedenle yalnızca numaranın çalışıyor olması, güven için yeterli değildir.

Arama sonuçlarında görülen yorumlara da temkinli yaklaşmak gerekir. Çok kısa, abartılı ve birbirine benzeyen yorumlar genellikle gerçek kullanıcı deneyimi izlenimi vermek için eklenir. “Kesinlikle güvenilir”, “sorunsuz hizmet”, “hiç düşünmeyin” gibi aşırı net ifadeler, özellikle hassas alanlarda dikkatle değerlendirilmelidir. Gerçek yorumlar genellikle daha ölçülü, daha ayrıntılı ve bazen küçük eleştiriler içerir. Her şeyin kusursuz anlatıldığı sayfalar, çoğu zaman fazla cilalıdır.

En yaygın dolandırıcılık yöntemi: ön ödeme tuzağı

Bu tür aramalarda en çok karşılaşılan dolandırıcılık biçimi ön ödeme talebidir. Karşı taraf önce güven verici bir konuşma yapar, ardından “kapora”, “ulaşım ücreti”, “güvenlik bedeli”, “rezervasyon ücreti” ya da “otel giriş masrafı” gibi gerekçelerle para ister. Miktar genellikle çok yüksek başlamaz. 300 TL, 500 TL, 1.000 TL gibi nispeten yönetilebilir görünen tutarlar seçilir. Amaç, kişinin fazla düşünmeden ödeme yapmasını sağlamaktır.

Ödeme yapıldıktan sonra senaryo değişir. Bazen “eksik gönderdiniz” denir, bazen “sistemde görünmedi” bahanesi kullanılır, bazen de başka bir kişi devreye girerek daha fazla para ister. Bazı dolandırıcılar, mağdurun ilk ödemeyi yaptığı psikolojik eşiği kullanır. Kişi zaten para gönderdiği için “madem başladım, belki bu son ödemedir” diye düşünebilir. Bu davranış, dolandırıcılık literatüründe sık görülen bir baskı alanıdır. Kayıp büyüdükçe kişi hatasını kabul etmekte zorlanır ve daha fazla para gönderebilir.

Ön ödeme tuzağının tehlikeli tarafı yalnızca para kaybı değildir. Banka dekontu, ad soyad, telefon numarası ve bazen konum bilgisi de karşı tarafa geçmiş olur. Bu bilgiler daha sonra tehdit ya da şantaj için kullanılabilir. Özellikle açıklama kısmına yazılan ifadeler, mağdurun aleyhine çevrilebilir. Bu nedenle herhangi bir ödeme yapmadan önce, bunun sadece maddi değil, kişisel veri riski doğuracağını da düşünmek gerekir.

Diyarbakır’da yaşayan biri için yerel çevre faktörü de önemlidir. Şehir büyük olsa da sosyal çevreler çoğu zaman tahmin edilenden daha bağlantılıdır. Dolandırıcılar bazen “seni tanıyoruz”, “ailene ulaşırız”, “iş yerine göndeririz” gibi tehditler savurur. Çoğu zaman ellerinde gerçek bir güç yoktur, ama panik yaratmayı hedeflerler. Panik, dolandırıcının en sevdiği zemindir.

Fotoğraf ve profil doğrulamada yapılan hatalar

İnternette fotoğraf doğrulamak artık eskiye göre daha zor. Çünkü görseller farklı platformlardan alınabiliyor, filtrelenebiliyor, yüzü kısmen kapatılabiliyor ya da yapay biçimde değiştirilebiliyor. Yine de bazı temel dikkat noktaları vardır. Aynı fotoğrafın farklı şehirlerde, farklı isimlerle kullanılması ciddi bir uyarı işaretidir. Bir profilde Diyarbakır yazarken aynı görselin başka bir yerde Ankara, Antalya veya Gaziantep adıyla çıkması, profilin sahte olma ihtimalini güçlendirir.

Görsel arama araçları bazen yardımcı olur, fakat kesin sonuç vermez. Dolandırıcılar fotoğrafı kırpar, ayna görüntüsüne çevirir, üzerine yazı ekler veya kaliteyi düşürür. Bu küçük değişiklikler, basit arama sistemlerinin eşleşme bulmasını zorlaştırabilir. Bu yüzden sadece görsel arama sonucuna güvenmek doğru değildir.

Profil metinleri de ipucu verir. Çok genel ifadeler, her şehre uyacak şekilde yazılmış tanıtımlar, aşırı abartılı vaatler ve sürekli tekrar eden kalıplar dikkat çekmelidir. Gerçek bir yerel bilgi neredeyse hiç yoksa, “Diyarbakır” kelimesi yalnızca anahtar kelime gibi duruyorsa, metin muhtemelen arama motoru için hazırlanmıştır. Özellikle “diyarbakır escort bayan” ifadesinin doğal olmayan şekilde sık kullanıldığı sayfalar, kullanıcıdan çok algoritmayı hedefler.

Bir de tersine fazla profesyonel görünen profiller vardır. Stüdyo kalitesinde fotoğraflar, marka diliyle yazılmış tanıtımlar, kusursuz sayfa düzeni ve çok hızlı yanıt veren hesaplar ilk bakışta güven verebilir. Fakat dolandırıcı ağları da artık amatör değildir. Bazı ekipler, çağrı merkezi düzeninde çalışır gibi farklı numaralardan mesajlaşır, hazır metinler kullanır ve kullanıcıyı belirli ödeme adımlarına yönlendirir. Güven, görüntüden değil tutarlılıktan anlaşılır.

İletişim sırasında kırmızı bayraklar

Mesajlaşma aşaması, riskleri erken fark etmek için en önemli yerdir. Dolandırıcılar genellikle hızlı karar aldırmaya çalışır. “Şu an uygunum”, “birazdan dolacağım”, “son kez yazıyorum”, “hemen kapora at” gibi baskı cümleleri bunun örneğidir. Acele ettirilen kişi daha az soru sorar, daha az araştırır ve daha kolay hata yapar.

İletişimde dikkat edilmesi gereken bazı işaretler özellikle belirgindir:

1. Daha ilk dakikalarda para talep edilmesi veya ödeme yapılmadan hiçbir bilgi verilmeyeceğinin söylenmesi.
2. Görüşme, kimlik, konum ya da kişisel bilgi paylaşımı konusunda tek taraflı baskı kurulması.
3. Sürekli farklı kişilerin yazması, numaranın veya hesabın kısa sürede değişmesi.
4. Sorulara net yanıt verilmemesi, hazır metinlerle geçiştirme yapılması.
5. Tehdit, hakaret, suçlama veya mahrem bilgileri yayma imasıyla para istenmesi.

Bu işaretlerden biri bile dikkat gerektirir. Birkaçının aynı anda görülmesi halinde iletişimi sürdürmek genellikle riski büyütür. Özellikle tehdit içeren konuşmalarda pazarlık yapmaya çalışmak çoğu zaman fayda sağlamaz. Dolandırıcı, mağdurun korktuğunu anladıkça daha fazlasını talep eder.

Mesajlaşmalarda sesli arama ya da görüntülü doğrulama istenmesi de mutlak çözüm değildir. Çünkü karşı taraf kısa, belirsiz, yüzü net göstermeyen ya da önceden hazırlanmış içerikler kullanabilir. Ayrıca görüntülü görüşme sırasında ekran kaydı alınıp sonradan şantaj malzemesi yapılması da mümkündür. Bu nedenle “görüntülü konuştum, o halde güvenlidir” düşüncesi tek başına yeterli değildir.

Şantaj ve tehdit durumunda panikle para göndermemek gerekir

Bu alandaki dolandırıcılıklar yalnızca sahte ilanlarla sınırlı değildir. Bazı kişiler iletişim kurduktan sonra mağduru korkutarak para almaya çalışır. “Ailene mesaj atacağız”, “sosyal medya hesaplarına yazacağız”, “polisiz”, “avukatız”, “çete bağlantımız var” gibi ifadeler kullanılabilir. Bazen sahte resmi evrak görselleri, sahte kimlik fotoğrafları veya sahte avukat kartları gönderilir. Amaç, mağdurun düşünmeden ödeme yapmasıdır.

Bu tür durumlarda ilk refleks genellikle konuşmayı yumuşatmak ya da para göndererek meseleyi kapatmaktır. Fakat pratikte para göndermek çoğu zaman tehdidi bitirmez. Aksine, mağdurun ödeme yapabileceğini gösterir. İlk ödeme sonrası “son bir işlem kaldı”, “dosya kapatma ücreti”, “ekip susturma parası” gibi yeni talepler gelebilir.

Tehdit mesajlarını silmemek önemlidir. Ekran görüntüsü almak, numaraları kaydetmek, ödeme taleplerini belgelemek ve mümkünse konuşmanın tarih saat bilgisini korumak gerekir. Kişi kendini fiziksel tehlikede hissediyorsa yerel kolluk birimlerine başvurmalıdır. Şantaj, tehdit ve kişisel verilerin hukuka aykırı kullanımı ciddi konulardır. Utanç duygusu, dolandırıcıların en çok kullandığı baskı aracıdır. Oysa mağduriyetin bildirilebilmesi için olayın eksiksiz belgelenmesi gerekir.

Burada ince bir ayrım vardır. Her rahatsız edici konuşma gerçek bir tehlike anlamına gelmez, fakat her tehdidi de hafife almak doğru değildir. Tehdidin içeriği, karşı tarafın sahip olduğu gerçek bilgiler, fiziksel konum bilgisi, ödeme geçmişi ve iletişim süresi birlikte değerlendirilmelidir. Panik yerine kayıt tutmak, iletişimi sınırlamak ve gerekirse profesyonel destek almak daha sağlıklı bir yoldur.

Kişisel veri paylaşımı küçük bir ayrıntı değildir

Birçok kişi para göndermediği sürece güvende olduğunu düşünür. Oysa dolandırıcılık bazen doğrudan para talebiyle başlamaz. Önce ad, yaş, meslek, konum, sosyal medya hesabı, çalışılan yer veya araç plakası gibi bilgiler toplanır. Bu bilgiler tek başına önemsiz görünebilir; fakat bir araya geldiğinde kişinin kimliğini ve çevresini ortaya çıkarabilir.

Telefon numarası da güçlü bir veridir. Numara üzerinden mesajlaşma uygulamalarındaki profil fotoğrafına, kullanıcı adına, bazen sosyal medya bağlantılarına ulaşılabilir. Kişi aynı numarayı işinde, ailesiyle iletişimde ve bankacılık işlemlerinde kullanıyorsa risk daha da artar. Bu yüzden hassas aramalarda kullanılan iletişim kanalının kişinin ana kimliğiyle ne kadar bağlantılı olduğu iyi düşünülmelidir.

Konum paylaşımı ayrıca hassas bir konudur. “Yakında mısın?”, “hangi oteldesin?”, “hangi semttesin?” gibi sorular masum görünebilir, fakat dolandırıcıya baskı kurma imkanı verir. Kişi bir otel adı, apartman adı veya iş yeri çevresi paylaştığında, karşı taraf bu bilgiyi tehdit için kullanabilir. Diyarbakır gibi belirli bölgelerde herkesin birbirini tanıdığı sosyal çevrelerde bu risk daha belirgin hissedilir.

Kimlik fotoğrafı ya da resmi belge paylaşımı ise kesinlikle ayrı değerlendirilmelidir. Hiçbir gayriresmi iletişimde kimlik, ehliyet, pasaport, banka kartı veya yüzle birlikte belge fotoğrafı gönderilmemelidir. Bu belgelerle sahte hesap açma, tehdit, borçlandırma girişimi ya da başka dolandırıcılıklara zemin hazırlanabilir. Bir belgenin üzerine “sadece doğrulama içindir” yazmak bile riski tamamen ortadan kaldırmaz.

Ödeme araçları ve iz bırakma meselesi

Dolandırıcılar çoğu zaman hızlı ve geri alınması zor ödeme yöntemlerini tercih eder. Banka havalesi, EFT, FAST, kripto para, dijital cüzdan, hediye kartı kodu veya üçüncü kişi hesabına gönderim gibi seçenekler gündeme gelebilir. Özellikle açıklama yazılmaması istenir ya da açıklamaya alakasız bir ifade yazdırılır. Bu, hem izleri bulanıklaştırmak hem de mağdurun sonradan itirazını zorlaştırmak için yapılır.

Banka hesabının başka bir kişiye ait olması sık görülen bir yöntemdir. Mesajla konuşulan kişi farklıdır, ödeme istenen IBAN farklı bir isimdedir. Bu durumda para, çoğu zaman “hesap kiralama” yoluyla kullanılan bir aracı hesaba gider. Hesabın sahibinin olayla bağlantısı bazen doğrudan, bazen dolaylı olabilir. Mağdur açısından ise paranın geri alınması zorlaşır.

Kripto para ve hediye kartı kodları daha risklidir. Bu yöntemlerde işlem geri döndürme imkanı çoğu durumda yoktur. Dolandırıcılar özellikle “banka istemiyorum, kod al gönder” gibi taleplerle kimliklerini gizlemeye çalışır. Hediye kartı kodu gönderildiğinde, kod saniyeler içinde kullanılabilir ve paranın takibi zorlaşır.

Bir ödeme yapılmışsa banka ile hızlı iletişime geçmek faydalı olabilir, ancak sonuç garanti değildir. İşlem henüz tamamlanmadıysa müdahale şansı olabilir. Tamamlanmış işlemlerde ise banka tek başına parayı iade edemez; hukuki süreç gerekebilir. Bu nedenle en etkili koruma, ödeme aşamasına hiç gelmemektir.

Yerel gerçeklik: Diyarbakır’da mahremiyet ve sosyal çevre baskısı

Diyarbakır, hem büyükşehir dinamiklerine hem de güçlü yerel bağlara sahip bir kenttir. Kayapınar’da yaşayan biri Sur’da, Yenişehir’de veya Bağlar’da çalışan insanlarla ortak çevrelere sahip olabilir. Üniversite, kamu kurumları, esnaf ilişkileri, aile bağları ve mahalle kültürü, kişisel bilgilerin yayılmasına dair kaygıyı artırabilir. Dolandırıcılar bu sosyal gerçeği çok iyi kullanır.

“Tanıdıklarına söyleriz” tehdidi, çoğu zaman teknik bir imkandan çok psikolojik baskıdır. Karşı tarafın gerçekten kime ulaşabileceği belirsizdir. Fakat mağdurun zihninde oluşan ihtimal, dolandırıcı için yeterlidir. Kişi itibar

kaygısıyla hızlı ödeme yapabilir, daha fazla bilgi verebilir veya konuşmayı uzatarak yeni açıklar yaratabilir.

Bu nedenle mahremiyet yönetimi, yalnızca gizlilik ayarı yapmak değildir. Hangi numarayla iletişim kurulduğu, profil fotoğrafının ne olduğu, sosyal medya hesaplarının telefon numarasıyla bulunup bulunmadığı, mesajlaşma uygulamalarında ad soyad görünüp görünmediği gibi ayrıntılar da önemlidir. Birçok kişi bu ayarları yıllarca değiştirmez. Oysa hassas bir iletişimde en küçük açık, büyük bir baskı aracına dönüşebilir.

Bunun yanında, yerel otel ve apart işletmeleri üzerinden kurulan sahte senaryolara da dikkat etmek gerekir. Dolandırıcılar bazen gerçek bir otel adını kullanır, ama otelle ilgileri yoktur. "Resepsiyona bilgi verildi", "oda hazır", "giriş için ödeme lazım" gibi ifadeler kullanabilirler. Kişi gerçekten o oteli aramadıkça bu bilgilerin doğruluğunu bilemez. Adı geçen işletmenin haberi bile olmayabilir.

Güvenlik için uygulanabilir bir kısa kontrol

Riskli bir arama ya da iletişimde, her ayrıntıyı kusursuz analiz etmek mümkün değildir. Yine de birkaç temel kontrol, birçok dolandırıcılık girişimini erken aşamada ele verir.

1. Ön ödeme isteniyorsa işlemi durdurun ve gerekçenin değişip değişmediğine bakın.
2. Profil fotoğrafını, metni ve telefon numarasını farklı kaynaklarda aratın.
3. Kişisel bilgi, kimlik belgesi, konum veya sosyal medya hesabı paylaşmayın.
4. Baskı, acele ettirme veya tehdit varsa konuşmayı uzatmayın.
5. Şüpheli mesajları silmeden belgeleyin ve gerekirse resmi destek alın.

Bu kontrol listesi mutlak güvenlik sağlamaz, fakat karar hızını düşürür. Dolandırıcılıkların çoğu hızla çalışır. Karşı taraf acele ettirirken siz yavaşlarsanız, senaryodaki açıkları görme ihtimaliniz artar.

Sahte yorumlar ve ilan ağları nasıl anlaşılır?

Sahte ilan ağları genellikle aynı dil yapısını kullanır. Metinlerde benzer cümleler, aynı sıfatlar, aynı vaatler ve aynı iletişim yönlendirmeleri bulunur. Farklı isimlerle açılmış profillerde bile yazım hataları aynıysa, bu önemli bir ipucudur. Bir kişinin kendini tanıtma biçimi doğal olarak benzersiz olur; kopya ağlarda ise metinler üretim bandından çıkmış gibi durur.

Yorumlar konusunda da ölçü önemlidir. Gerçek kullanıcı yorumları, özellikle hassas konularda fazla ayrıntıya girmez ama tamamen reklam metni gibi de yazılmaz. Her yorumun aynı uzunlukta olması, aynı kelimeleri tekrar etmesi, kısa aralıklarla eklenmiş görünmesi veya hiç olumsuz deneyim içermemesi şüphe yaratır. Bir sayfada yıllardır hizmet verildiği iddia ediliyor ama tüm yorumlar son birkaç güne aitse, bu da sorgulanmalıdır.

İlan sitelerindeki "editör onaylı" ya da "kontrollü profil" ifadeleri bazen yalnızca site içi bir pazarlama unsurudur. Bağımsız bir doğrulama mekanizması, resmi kayıt veya açık sorumluluk yoksa bu ibarelerin koruyuculuğu sınırlıdır. Bazı siteler yalnızca ilan yayıncılığı yapar ve içerikteki kişilerin doğruluğunu denetlemez. Kullanıcı bunu bilmeden hareket ettiğinde, platforma duyduğu güveni yanlış kişilere aktarır.

Arama motorunda aynı telefon numarasını tırnak içinde aramak bazen işe yarar. Numara farklı isimlerle, farklı şehirlerde veya şikayet sayfalarında geçiyorsa dikkat etmek gerekir. Fakat hiçbir sonuç çıkmaması da güvenilirlik kanıtı değildir. Yeni kullanılan bir hat, henüz internette iz bırakmamış olabilir. Dijital iz yokluğu, temiz geçmiş anlamına gelmez.

Hukuki belirsizlikleri hafife almamak gerekir

Türkiye'de fuhuş, aracılık, yer temini, insan ticareti, tehdit, şantaj ve kişisel verilerin kötüye kullanılması gibi konular farklı hukuki başlıklar altında değerlendirilebilir. Bireysel davranışların hangi hukuki sonuca yol açacağı somut olaya göre değişir. Bu nedenle internet üzerinden yapılan her iletişimde sadece dolandırıcılık değil, hukuki risk de düşünülmelidir.

Özellikle üçüncü kişiler tarafından organize edilen ilanlar, aracılık şüphesi doğurabilir. Bir numaradan farklı kişiler adına yönlendirme yapılması, "ekip", "ajans", "menajer" gibi ifadeler kullanılması ya da ödeme için başka hesaplara yönlendirme yapılması, konuyu daha karmaşık hale getirir. Kullanıcı çoğu zaman yalnızca bireysel bir iletişim kurduğunu sanır, fakat karşısında organize bir yapı olabilir.

Yaş doğrulama konusu da çok kritiktir. İnternette beyan edilen yaşa güvenmek ciddi risk taşır. Fotoğraf, ses veya yazışma üzerinden yaş tespiti güvenilir değildir. Bu alandaki en ağır hukuki ve etik risklerden biri, kişinin yaşı diyarbakır eskort bayan hakkında yanlış veya sahte bilgi verilmesidir. Böyle bir belirsizlik varsa iletişimi sürdürmemek en güvenli yaklaşımdır.

Hukuki sorunlar yalnızca karşı tarafın şikayetiyle de sınırlı değildir. Otel, apart, çevredekiler, ödeme kayıtları, mesajlaşma içerikleri ve dijital izler farklı süreçlerde gündeme gelebilir. Bu yüzden "nasıl olsa internetten konuşuyorum" düşüncesi yanıltıcıdır. Dijital iletişim, çoğu zaman sanıldığından daha kalıcı izler bırakır.

Dolandırıcılığa uğrandıysa ne yapılmalı?

Bir kişi para göndermiş, tehdit almış ya da kişisel bilgilerini paylaşmış olabilir. Bu noktada kendini suçlamak yerine zararı sınırlamaya odaklanmak gerekir. İlk adım, iletişimi kontrolsüz biçimde sürdürmemektir. Dolandırıcıya uzun açıklamalar yapmak, yalvarmak, hakaret etmek veya pazarlığa girmek genellikle durumu düzeltmez. Karşı tarafın amacı duygusal tepkiyi yöneterek daha fazla çıkar sağlamaktır.

Ödeme yapıldıysa dekontlar saklanmalıdır. Banka müşteri hizmetleriyle hızlıca görüşülmeli, işlemin durumu sorulmalı ve şüpheli işlem bildirimi yapılmalıdır. Para geri dönmeyebilir, fakat kayıt oluşturmak önemlidir. Tehdit mesajları, telefon numaraları, kullanıcı adları, profil bağlantıları ve ***Daha fazla bilgi bulabilirsiniz*** varsa ses kayıtları hukuka uygun şekilde muhafaza edilmelidir. Ekran görüntülerinde tarih ve saat görünmesi faydalı olur.

Şantaj veya tehdit varsa resmi mercilere başvurmak düşünülmelidir. Birçok mağdur, konunun mahremiyeti nedeniyle başvuru yapmaktan çekinir. Fakat dolandırıcılar tam da bu çekingenlikten güç alır. Olayın detayları utandırıcı görünse bile tehdit ve şantaj ayrı bir suç niteliği taşıyabilir. Profesyonel hukuki danışmanlık almak, özellikle yüksek para kaybı veya ciddi tehdit durumlarında daha sağlıklı karar verilmesini sağlar.

Kişisel veri paylaşılmışsa ek önlemler gerekir. Sosyal medya gizlilik ayarları gözden geçirilmeli, telefon numarasıyla bulunabilirlik kapatılmalı, mesajlaşma uygulamalarındaki profil bilgileri sınırlandırılmalı, gerekirse önemli hesapların şifreleri değiştirilmelidir. Banka kartı ya da kimlik görüntüsü paylaşıldıysa ilgili kurumlarla iletişime geçmek gerekebilir. Her olay aynı ağırlıkta değildir, ama riskin ciddiyetine göre hızlı davranmak zarar azaltır.

Güvenli davranış, yalnızca şüphelenmek değil sınır koymaktır

Dolandırıcılıktan korunma çoğu zaman teknik araçlarla anlatılır: numara sorgula, fotoğraf arat, siteyi kontrol et, ödeme yapma. Bunlar önemlidir, fakat asıl mesele sınır koyabilmektir. Karşı taraf ne kadar ikna edici konuşursa konuşsun, kişisel bilgi paylaşmama sınırı net olmalıdır. Ön ödeme yapmama sınırı net olmalıdır. Tehdit karşısında para göndermeme sınırı net olmalıdır.

İnternet üzerindeki riskli alanlarda dolandırıcılar insanların merakını, yalnızlığını, aceleciliğini, mahremiyet kaygısını ve bazen de suçluluk duygusunu kullanır. Bu duygular insani duygulardır. Sorun, bu duygularla karar verildiğinde ortaya çıkar. Daha sağlıklı yaklaşım, iletişimi yavaşlatmak ve her talebi ayrı değerlendirmektir. Bir kişi gerçekten

güvenilirse, makul sorular karşısında saldırganlaşmaz. Sürekli baskı kuran, para isteyen, bilgi isteyen veya tehdit eden biriyle güven ilişkisi kurulamaz.

“Escort bayan diyarbakır” gibi aramalar yapan bir kullanıcının karşılaştığı her profilin arkasında gerçek bir kişi olduğunu varsaymak hatadır. Bazıları tamamen sahte olabilir, bazıları çalıntı görsellerle hazırlanmış olabilir, bazıları da dolandırıcı ağlarının yem profili olarak kullanılabilir. Aynı şekilde “Bayan escort diyarbakır” ifadesiyle açılan sayfaların yerel görünmesi de yeterli değildir. Yer adı eklemek, sahte bir ilanı gerçek yapmaz.

En sağlam koruma, riskli zemini erken fark edip işlem yapmamaktır. Para göndermemek, belge paylaşmamak, konum vermemek, tehdit mesajlarını kaydetmek ve panikle hareket etmemek, çoğu olayda zararı ciddi biçimde azaltır. Dijital ortamda güven, karşı tarafın söylediği şeylerden çok sizin koruduğunuz sınırlarla ilgilidir. Bu sınırlar net olduğunda, dolandırıcının hareket alanı daralır.