Dijital ortamda yapılan yetişkin içerikli aramalar, çoğu kişinin sandığından daha fazla iz bırakır. Arama motoruna yazılan birkaç kelime, ziyaret edilen bir ilan sayfası, mesajlaşma uygulamasında açılan kısa bir sohbet veya indirilen bir görsel, tek başına önemsiz görünse bile bir araya geldiğinde kişisel mahremiyet açısından ciddi risk doğurabilir. "Diyarbakır escort bayan" gibi yerel ve hassas nitelikteki aramalarda bu risk daha belirgin hale gelir, çünkü hem konum hem de niyet hakkında fikir veren bir veri izi oluşur.

Bu yazının amacı herhangi bir yasa dışı faaliyeti teşvik etmek değildir. Ama gerçek şu ki insanlar internette yetişkin hizmetleri, arkadaşlık, özel görüşme veya benzer başlıklarda arama yapıyor. Bu alanlarda dolandırıcılık, şantaj, kimlik avı, sahte profil, zararlı bağlantı ve kişisel veri sızıntısı gibi riskler sık görülüyor. Dijital güvenlik bakış açısıyla mesele, kişinin ne aradığına dair ahlaki bir değerlendirme yapmak değil, çevrimiçi ortamda kendisini nasıl koruyacağını bilmesidir.

Profesyonel bir perspektiften bakıldığında en temel ilke şudur: Hassas bir arama yapıyorsanız, sıradan bir ürün fiyatı araştırıyormuş gibi davranamazsınız. Kullandığınız cihaz, tarayıcı, ödeme yöntemi, mesajlaşma dili, paylaştığınız fotoğraf ve hatta yazım tarzınız bile iz bırakabilir. Güvenli davranış, tek bir uygulama indirerek sağlanmaz. Birkaç küçük alışkanlığın birlikte uygulanması gerekir.

Hassas aramalarda risk nerede başlar?

Risk çoğu zaman ilk mesajla başlamaz. Daha erken başlar. Tarayıcının geçmişinde, otomatik tamamlama kayıtlarında, çerezlerde, reklam takip sistemlerinde ve arama motorunun kişiselleştirme verilerinde başlar. Bir kişi "Diyarbakır escort bayan" gibi bir kelime öbeğini arattığında, sadece bir sonuç listesi görmez. Aynı zamanda cihazı ve hesabı o ilgi alanıyla ilişkilendirilebilir.

Bu noktada birçok kişi "gizli sekme açtım, sorun olmaz" diye düşünür. Gizli sekme, aynı cihazı kullanan başka birinin tarayıcı geçmişini görmesini zorlaştırır, fakat internet servis sağlayıcısını, ziyaret edilen siteleri, iş yeri ağ yöneticisini veya kötü niyetli web izleyicilerini tamamen devre dışı bırakmaz. Gizli sekme bir mahremiyet aracıdır, anonimlik kalkanı değildir.

Daha pratik bir örnek verelim. Evde ortak kullanılan bir bilgisayarda hassas bir arama yapıldıysa ve tarayıcıda otomatik doldurma açıksa, birkaç gün sonra başka biri adres çubuğuna benzer bir harf yazdığında önceki aramalar veya ziyaret edilen sayfalar öneri olarak çıkabilir. Benzer şekilde ortak kullanılan bir Google hesabı varsa, telefonda yapılan arama dizüstü bilgisayardaki geçmişe yansıyabilir. Bu durum teknik olarak karmaşık değildir, ama çoğu mahremiyet ihlali tam da bu basit senaryolardan doğar.

Yerel aramalarda konum verisinin önemi

Diyarbakır gibi belirli bir şehir adıyla yapılan aramalar, mahremiyet açısından genel aramalardan daha hassastır. Çünkü konum bilgisi, kişinin hareket alanını ve muhtemel fiziksel çevresini daraltır. Bir profille yazışırken mahalle, otel, iş yeri, plaka, yakın çevredeki bilinen noktalar veya günlük rutin hakkında verilen küçük bilgiler, karşı tarafın kişiyi tahmin etmesine yardımcı olabilir.

Konum verisi yalnızca kişinin kendi yazdığı mesajlardan çıkmaz. Fotoğrafların EXIF verileri, yani fotoğrafın çekildiği cihaz, tarih ve bazen konum bilgisi gibi teknik kayıtlar da risk oluşturabilir. Modern mesajlaşma uygulamalarının çoğu fotoğraf meta verilerini kısmen temizler, fakat buna güvenmek doğru değildir. Özellikle dosya olarak gönderilen görsellerde veya bazı web formlarına yüklenen fotoğraflarda bu veriler korunabilir.

Harita bağlantısı paylaşmak da dikkat ister. Bir buluşma noktası, otel adı veya ev adresine yakın bir konum, tek seferlik bir bilgi gibi görünse de ileride şantaj veya taciz için kullanılabilir. Bu yüzden hassas iletişimlerde tam adres, evin dış cephesi, araç plakası, apartman adı, iş yeri lokasyonu ve düzenli gidilen mekanlar paylaşılmamalıdır. Güvenlik, sadece dijital değil, fiziksel mahremiyeti de kapsar.

Sahte ilanlar ve dolandırıcılık kalıpları

Yetişkin hizmetleriyle ilişkili aramalarda sahte ilan sayısı yüksektir. Bunun nedeni basittir: Kullanıcılar mahremiyet endişesi nedeniyle şikayet etmekten çekinebilir. Dolandırıcılar da bu çekingenliği kullanır. “Kapora gönder, sonra konum atacağım” modeli en bilinen yöntemlerden biridir. Küçük görünen bir miktarla başlar, ardından ek ücret, güvenlik bedeli, ulaşım ücreti veya iptal cezası gibi gerekçelerle devam eder. Para gönderildikten sonra profil kaybolur veya mağdur daha fazla ödeme yapmaya zorlanır.

Bir diğer yaygın yöntem şantajdır. Kişiden yüz fotoğrafı, kimlik görüntüsü, sosyal medya hesabı veya telefon rehberine erişim isteyen profiller ciddi risk taşır. Bazı dolandırıcılar kısa bir yazışmadan sonra kişinin ailesine, iş yerine veya arkadaşlarına ulaşacağını söyleyerek para ister. Bu tür tehditler özellikle hassas arama yapan kişiler üzerinde psikolojik baskı kurmak için tasarlanır.

Burada dikkat edilmesi gereken nokta, dolandırıcının her zaman amatör görünmediğidir. Bazı sahte profiller oldukça düzenli hazırlanır. Fotoğraflar profesyonel olabilir, metinler inandırıcı yazılmış olabilir, hatta yerel semt isimleri kullanılarak gerçeklik hissi yaratılabilir. Fakat tutarlı görünen bir profil, güvenilirlik kanıtı değildir. İnternette fotoğraf kopyalamak, sahte yorum üretmek ve geçici telefon numarası almak çok kolaydır.

İlk temas öncesi kısa güvenlik kontrolü

Hassas bir iletişime geçmeden önce birkaç dakikalık kontrol, sonradan yaşanabilecek büyük sorunları önleyebilir. Bu kontrolün amacı karşı tarafı “kesin güvenilir” ilan etmek değildir. Ama bariz riskleri ayıklamak mümkündür.

1. Profil fotoğraflarının tersine görsel aramayla başka sitelerde kullanılıp kullanılmadığını kontrol edin.
2. İlan metninde aşırı acele ettiren, kapora isteyen veya tehditkar bir dil olup olmadığına bakın.
3. Kişisel numaranız yerine mümkünse ayrı ve mahremiyet odaklı bir iletişim kanalı kullanın.
4. Kimlik, yüz fotoğrafı, iş yeri bilgisi veya ev adresi gibi geri alınamaz verileri paylaşmayın.
5. Bağlantılara tıklamadan önce alan adını inceleyin, kısaltılmış linklere özellikle temkinli yaklaşın.

Bu maddeler basit görünebilir, fakat sahadaki çoğu dolandırıcılık bu basit eşikleri aşan kişiler üzerinden yürür. Acele eden, merak eden, utandığı için yardım istemeyen veya "bir şey olmaz" diyen kullanıcı hedef haline gelir. Dijital güvenlikte küçük tereddütler çoğu zaman faydalıdır. Bir şey fazla hızlı ilerliyorsa, genellikle yavaşlamak gerekir.

Telefon numarası ve mesajlaşma uygulamaları

Kişisel telefon numarası, internette sanıldığından daha güçlü bir kimlik bilgisidir. Numara üzerinden sosyal medya hesapları bulunabilir, mesajlaşma uygulamalarındaki profil fotoğrafı görülebilir, bazı veri sızıntılarında ad soyadla eşleşebilir. Ayrıca numara bir kez kötü niyetli kişilerin eline geçtiğinde *Diyarbakır Escort Bayan* istenmeyen arama, taciz, tehdit veya spam mesajları başlayabilir.

Bu yüzden hassas aramalarda ana telefon numarasını kullanmak iyi bir fikir değildir. Bazı kullanıcılar ikinci bir hat veya yalnızca bu tür hassas iletişimler için ayrılmış bir cihaz tercih eder. Bu herkes için pratik olmayabilir, fakat en azından mesajlaşma uygulamalarında profil fotoğrafını, görünen adı ve durum bilgisini sınırlamak gerekir. WhatsApp gibi uygulamalarda "son görülme", profil fotoğrafı ve hakkında kısmı yalnızca rehberdeki kişilere gösterilecek şekilde ayarlanabilir. Rehbere kaydedilmeyen kişilerden gelen mesajlara karşı da temkinli olmak gerekir.

Telegram, Signal veya benzeri uygulamalar farklı mahremiyet seçenekleri sunar, fakat hiçbir uygulama kötü kararları telafi edemez. Kullanıcı adı ile iletişim kurmak, telefon numarasını gizlemek ve ekran görüntüsü riskini düşünmek önemlidir. Unutulmaması gereken bir başka nokta da şudur: Uçtan uca şifreleme, mesajın iletim sırasında okunmasını zorlaştırır, fakat karşı taraf ekran görüntüsü alırsa veya başka bir cihazla fotoğrafını çekerse mesajın gizliliği biter.

Fotoğraf, ses kaydı ve kişisel belgelerde geri dönüş yoktur

Dijital dünyada bazı veriler paylaşıldıktan sonra geri alınamaz. Yüz fotoğrafı, kimlik kartı, pasaport, ehliyet, öğrenci kartı, banka dekontu, otel rezervasyonu ve uçak bileti gibi belgeler bunların başında gelir. Bir dolandırıcı için bu belgeler yalnızca bilgi değildir, baskı aracıdır. Kişinin adını, soyadını, T.C. Kimlik numarasını, adresini veya doğum tarihini öğrenmek, kimlik avı girişimlerini kolaylaştırabilir.

Ses kayıtları da küçümsenmemelidir. Kısa bir sesli mesaj bile kişinin kimliğini ele verebilir. Yerel ağız, arka plandaki sesler, anonslar, araç içi gürültü veya iş ortamına ait ipuçları kişiyi tanınabilir hale getirebilir. Hassas iletişimlerde yazılı mesaj bile risk taşırken, ses ve görüntü paylaşımı bu riski büyütür.

Fotoğraf paylaşımı gerekiyorsa yüzü, ayırt edici dövme, takı, kıyafet logosu, ev içi detaylar ve pencere manzarası gibi unsurları düşünmek gerekir. Bir fotoğrafta görünen küçük bir duvar tablosu ya da ofis kartı, kişiyi beklenmedik şekilde tanınabilir kılabilir. Profesyonel güvenlik yaklaşımı, "bu bilgi tek başına zararsız mı?" sorusuyla yetinmez. "Bu bilgi başka verilerle birleşince neye dönüşür?" diye sorar.

Ödeme güvenliği ve finansal izler

Hassas aramalarda finansal izler ayrı bir risk alanıdır. Banka havalesi, FAST, kredi kartı ödemesi veya dijital cüzdan kullanımı farklı düzeylerde kayıt bırakır. Bir banka dekontunda ad soyad, IBAN, açıklama alanı, işlem saati ve tutar görülür. Bu bilgiler karşı tarafın eline geçtiğinde hem mahremiyet hem de şantaj riski oluşabilir.

Kapora talepleri özellikle dikkat gerektirir. Dolandırıcıların sık kullandığı yöntemlerden biri küçük tutarlı ön ödeme istemektir. "Sadece güven için", "iptal olmasın diye", "yol parası" veya "oda rezervasyonu" gibi gerekçelerle

istenen ödemeler çoğu zaman geri dönmez. Ödeme yapıldıktan sonra yeni bir talep gelir. Kullanıcı geri çekilmek istediğinde ise tehdit başlar.

Burada yasal çerçeveyi de unutmamak gerekir. Türkiye'de fuhuşla bağlantılı aracılık, yer temini, teşvik veya benzeri eylemler ciddi hukuki sonuçlar doğurabilir. İnternet üzerinden yapılan yazışmalar ve para transferleri, gerektiğinde delil niteliği taşıyabilir. Bu nedenle konu sadece mahremiyet meselesi değildir. Kişinin hukuki riskleri de gözetmesi gerekir. Herhangi bir şüpheli durumda ödeme yapmamak, kişisel bilgi vermemek ve iletişimi kesmek en sağlıklı yaklaşımdır.

Zararlı bağlantılar, sahte doğrulama sayfaları ve uygulama tuzakları

Sahte profillerin kullandığı bir başka yöntem de bağlantı göndermektir. Bu bağlantılar bazen "fotoğraflarım burada", "konum buradan açılıyor", "güvenlik doğrulaması yap", "yaş doğrulama gerekli" gibi mesajlarla iletilir. Kullanıcı linke tıkladığında sahte bir giriş sayfasına, zararlı yazılım indirme ekranına veya kredi kartı bilgisi isteyen bir forma yönlendirilebilir.

Alan adı kontrolü burada önemlidir. Gerçek bir hizmete benzetilen ama harfleri değiştirilmiş alan adları sık kullanılır. Örneğin popüler bir platformun adına fazladan bir harf eklenir veya ".com" yerine farklı bir uzantı kullanılır. Telefonda küçük ekranda bu farklar kolayca kaçabilir. Kısaltılmış bağlantılar da risklidir, çünkü tıklamadan önce nereye gideceğinizi net göremezsiniz.

Uygulama indirme konusunda da dikkatli olmak gerekir. Resmi uygulama mağazaları dışında gönderilen APK dosyaları, özellikle Android cihazlarda ciddi risk oluşturur. Bu dosyalar rehberinize, kameranıza, mikrofonunuza, konumunuza veya dosyalarınıza erişmeye çalışabilir. Bir kez izin verdiğinizde, cihazınızdaki özel bilgiler kopyalanabilir. Yetişkin içerikli vaatlerle yayılan zararlı yazılımlar yıllardır kullanılan bir taktiktir ve hâlâ etkilidir, çünkü kullanıcılar merak ve mahremiyet baskısıyla hızlı karar verir.

Cihaz ayarları: En zayıf halka çoğu zaman eldeki telefondur

Güvenli davranış sadece karşı tarafa güvenmemekle sınırlı değildir. Kendi cihazınızın güvenliği de belirleyicidir. Ekran kilidi olmayan bir telefon, bildirimleri kilit ekranında açık gösteren bir mesajlaşma uygulaması veya ortak kullanılan bir tablet, mahremiyet açısından açık kapı bırakır. Birçok kişi karmaşık şifrelerden kaçınır, fakat en az altı haneli güçlü bir PIN, biyometrik kilit ve otomatik kilit süresinin kısa tutulması temel güvenlik sağlar.

Bildirim içerikleri özellikle hassas yazışmalarda sorun yaratır. Telefon masadayken gelen bir mesajın tamamı ekranda görünüyorsa, dijital güvenliğin büyük bölümü boşa gider. Mesajlaşma uygulamalarında bildirim önizlemelerini kapatmak küçük ama etkili bir adımdır. Aynı şekilde galeri uygulamasında özel fotoğrafların otomatik bulut yedeklemesine gitmesi de istenmeyen sonuçlar doğurabilir. iCloud, Google Fotoğraflar veya benzeri servisler kullanılıyorsa hangi klasörlerin yedeklendiğini bilmek gerekir.

Tarayıcı tarafında çerezler, kayıtlı şifreler ve otomatik doldurma verileri düzenli temizlenmelidir. Hassas aramalar için ayrı bir tarayıcı profili kullanmak pratik bir yöntem olabilir. Bu profil, gündelik e-posta, sosyal medya ve iş hesaplarından ayrıldığında veri karışması azalır. VPN kullanımı bazı durumlarda ek mahremiyet sağlar, fakat ücretsiz ve güvenilmez VPN servisleri verileri toplayabilir. Güvenlik aracı seçerken "ücretsiz" olanın maliyetini sorgulamak gerekir.

Sosyal mühendislik: Teknikten çok psikoloji

Dolandırıcılık çoğu zaman teknik açıktan değil, insan davranışından yararlanır. Sosyal mühendislik, karşı tarafın acele etmesini, utanmasını, yalnız hissetmesini veya bir fırsatı kaçırmaktan korkmasını sağlar. Hassas aramalarda

bu yöntem daha etkilidir, çünkü kullanıcı genellikle konuyu çevresine açmak istemez. Dolandırıcı bunu bilir.

Tipik senaryo şöyle ilerler: Önce samimi bir dil kurulur, sonra güven oluşturulur, ardından küçük bir kişisel bilgi istenir. Telefon numarası, fotoğraf, konum, ödeme dekontu veya sosyal medya hesabı gibi bir veri alındığında baskı başlar. Tehditler bazen çok gerçekçi görünür, bazen de tamamen blöftür. Ancak panik anında kişi daha fazla bilgi ve para vererek durumu büyütebilir.

Bu noktada soğukkanlılık kritik önem taşır. Tehdit içeren mesajlara uzun açıklamalarla yanıt vermek, dolandırıcıya daha fazla malzeme sağlar. "Lütfen yapma", "ailem öğrenirse biterim" gibi cümleler, baskının işe yaradığını gösterir. Daha güvenli yaklaşım, iletişimi sınırlamak, ekran görüntüsü almak, ödeme yapmamak ve gerekiyorsa hukuki destek almaktır. Şantaj tehdidi suçtur ve mağdurun utanması, suçlunun avantajıdır.

Acil durumda ne yapılmalı?

Bir kişi kendisini dolandırıcılık, şantaj veya veri sızıntısı riski içinde bulduğunda hızlı ama kontrollü hareket etmelidir. Panikle tüm mesajları silmek çoğu zaman iyi fikir değildir, çünkü delil kaybolabilir. Önce kayıt almak, sonra hesap ve cihaz güvenliğini sağlamak gerekir.

1. Tehdit, ödeme talebi, profil bilgisi ve para transferiyle ilgili ekran görüntülerini zaman damgası görünecek şekilde kaydedin.
2. Karşı tarafa yeni bilgi, yeni fotoğraf veya yeni ödeme göndermeyin.
3. Hesap şifrelerinizi değiştirin, iki aşamalı doğrulamayı açın ve açık oturumları kapatın.
4. Bankanızla görüşerek şüpheli işlem ihtimalini bildirin, gerekirse kartları geçici olarak kapatın.
5. Ciddi tehdit, şantaj veya kişisel veri kullanımı varsa hukuki destek alın ve yetkili makamlara başvurun.

Bu adımların sırası olayın niteliğine göre değişebilir. Örneğin banka bilgisi paylaşıldıysa finansal önlem daha acil hale gelir. Sosyal medya hesabı ele geçirildiyse önce şifre ve oturum güvenliği sağlanmalıdır. Fiziksel adres paylaşılmış ve tehdit alınmışsa konu dijital mahremiyetin ötesine geçer, güvenli bir ortamda destek almak gerekir.

Yasal ve etik sınırları göz ardı etmemek

Dijital güvenlik yazılarında yalnızca teknik tavsiyelere odaklanmak kolaydır, fakat hassas yetişkin aramalarında hukuki ve etik boyutu atlamak eksik olur. Türkiye'de yetişkin hizmetleriyle bağlantılı faaliyetler, özellikle aracılık, organizasyon, yer sağlama, ilan verme veya başkasının bu yolla kazanç elde etmesini sağlama gibi durumlarda hukuki risk doğurabilir. İnternet üzerindeki içerikler ve mesajlaşmalar, kullanıcıların düşündüğünden daha kalıcıdır.

Ayrıca karşı tarafın yaşı, rızası, zorlanıp zorlanmadığı ve insan ticareti gibi ağır riskler dikkate alınmalıdır. Dijital ortamda görülen her profilin gerçek ve özgür iradeyle hareket eden bir yetişkine ait olduğunu varsaymak yanlıştır. Şüpheli bir durumda geri çekilmek yalnızca kişisel güvenlik açısından değil, etik sorumluluk açısından da önemlidir.

Rıza ve güvenlik, yetişkin ilişkilerinin temelidir. Karşı tarafı baskılayan, tehdit eden, görüntü isteyen, mahrem bilgileri kaydeden veya paylaşan davranışlar kabul edilemez. Mahremiyet hakkı tek taraflı değildir. Kişi kendi güvenliğini korurken başkalarının kişisel verilerine ve sınırlarına da saygı göstermelidir.

Arama motoru ve reklam izleri

Arama motorları yalnızca yazdığınız kelimeleri değil, davranış biçiminizi de değerlendirir. Hangi sonuçlara tıkladığınız, sayfada ne kadar kaldığınız, hangi reklamları gördüğünüz ve hangi cihazdan bağlandığınız gibi

sinyaller reklam sistemleri tarafından kullanılabilir. Bu nedenle hassas aramalardan sonra benzer reklamların görünmesi şaşırtıcı değildir. Ortak kullanılan bir cihazda bu durum mahremiyeti zedeleyebilir.

Kişiselleştirilmiş reklamları kapatmak, arama geçmişini silmek ve hassas oturumları ana hesaplardan ayrı yürütmek daha kontrollü bir ortam sağlar. Ancak burada da gerçekçi olmak gerekir. Arama geçmişini silmek, internet üzerindeki tüm kayıtları yok etmez. Yalnızca sizin hesabınızda veya cihazınızda görünen bazı izleri azaltır. Ziyaret edilen sitelerin kendi kayıtları, ağ düzeyindeki kayıtlar ve üçüncü taraf izleyiciler ayrı bir konudur.

Tarayıcı eklentileri de dikkatle seçilmelidir. Reklam engelleyici veya izleyici engelleyici araçlar faydalı olabilir, fakat bilinmeyen eklentiler tarayıcı geçmişine erişebilir. Güvenlik için yüklenen bir aracın kendisi veri toplayan bir kapıya dönüşebilir. Bu yüzden az sayıda, bilinen, güncel ve güvenilir araç kullanmak daha doğrudur.

Diyarbakır gibi şehir odaklı aramalarda sosyal çevre riski

Yerel aramalarda en hassas konu, dijital kimliğin fiziksel çevreyle kesişmesidir. Büyük şehirlerde bile sosyal çevreler sanıldığından küçüktür. Diyarbakır gibi güçlü sosyal bağların bulunduğu yerlerde, semt, meslek, araç, mekan ve ortak tanıdık bilgileri kişiyi hızla tanınabilir hale getirebilir. Bu nedenle yerel ayrıntı verirken ölçülü olmak gerekir.

Bir kişi yazışmada “şu otelin yakınındayım”, “şu kurumda çalışıyorum”, “akşam şu kafedeydim” gibi bilgiler verdiğinde bunları sıradan sohbet sanabilir. Fakat kötü niyetli biri bu parçaları birleştirerek kimlik tahmini yapabilir. Sosyal medya hesapları herkese açıksa iş daha ***Bu siteyi göz atın*** da kolaylaşır. Profil fotoğrafı, takip edilen yerel işletmeler, etiketlenen mekanlar ve arkadaş listesi, telefon numarasıyla birleştiğinde güçlü bir iz haritası oluşur.

Bu yüzden sosyal medya gizlilik ayarları da dijital güvenliğin parçasıdır. Herkese açık profil, hassas iletişimlerde riski büyütür. Eski paylaşımlardaki konum etiketleri, iş yeri bilgileri ve aile üyeleri görünür durumdaysa, dolandırıcının baskı alanı genişler. Mahremiyet ayarlarını yalnızca olay yaşandıktan sonra değil, önceden düzenlemek gerekir.

Gerçekçi güvenlik: Sıfır risk değil, bilinçli sınır

Dijital güvenlikte sıfır risk yoktur. En iyi araçları kullanan, ayrı cihazla iletişim kuran, VPN açan, fotoğraf paylaşmayan ve ödeme yapmayan biri bile tamamen görünmez olmaz. Ama amaç görünmezlik değildir. Amaç, gereksiz izleri azaltmak, kritik bilgileri korumak ve kötü niyetli kişilerin işini zorlaştırmaktır.

Bilinçli sınır koymak burada anahtar kavramdır. Hangi bilgiyi paylaşmayacağınızı önceden belirlemek, olay anında daha sağlam durmanızı sağlar. Ana telefon numaramı vermem, kimlik paylaşmam, kapora göndermem, yüz fotoğrafı iletmem, tehdit karşısında pazarlık yapmam gibi kararlar önceden alındığında sosyal mühendislik etkisini kaybeder.

“Diyarbakır escort bayan” gibi hassas aramalar yapan kişilerin en sık hatası, dijital mahremiyeti yalnızca yakalanmamak veya görünmemek olarak düşünmesidir. Oysa güvenlik daha geniştir. Dolandırılmamak, şantaja açık hale gelmemek, cihazını korumak, hukuki riskleri anlamak, karşı tarafın sınırlarına saygı göstermek ve fiziksel güvenliği tehlikeye atmamak aynı bütünün parçalarıdır.

Sağlam dijital alışkanlıklar gösterişli değildir. Çoğu zaman sıkıcı görünür. Linke hemen tıklamamak, kapora göndermemek, bildirim önizlemelerini kapatmak, fotoğraf meta verilerini düşünmek, arama geçmişini yönetmek ve şüpheli durumda durmak. Fakat hassas alanlarda güvenliği sağlayan şey tam da bu sıkıcı görünen alışkanlıklardır. Birkaç dakikalık dikkat, haftalarca sürebilecek bir krizi önleyebilir.