Diyarbakır'da dijital iletişim, gündelik hayatın sıradan bir parçası olmaktan çıktı; iş, aile, arkadaşlık, alışveriş, randevu, resmi işlemler ve sosyal çevre artık çoğu zaman ekran üzerinden ilerliyor. Sur'da bir esnafın müşterisiyle WhatsApp üzerinden yazışması, Kayapınar'da yaşayan bir öğrencinin çevrim içi ders grubuna katılması, Bağlar'da bir ailenin şehir dışındaki akrabalarıyla görüntülü konuşması, Yenişehir'de çalışan birinin banka işlemini telefondan yapması aynı geniş başlığın içinde yer alıyor: dijital iletişim.

Bu iletişim pratik görünür, hızlıdır, çoğu zaman da hayat kurtarır. Fakat hızın bedeli vardır. Yanlış kişiye gönderilen bir ekran görüntüsü, zayıf bir şifre, herkese açık Wi-Fi ağı üzerinden yapılan banka girişi, aceleyle tıklanan bir bağlantı veya fazla kişisel bilgi paylaşımı beklenmedik sorunlara yol açabilir. Diyarbakır gibi sosyal bağların güçlü olduğu, insanların birbirini mahalle, iş, okul ve akrabalık çevreleri üzerinden tanıdığı bir şehirde dijital hataların etkisi bazen çevrim dışı hayata da taşar.

Güvenli dijital iletişim, sadece teknik bilgiyle ilgili değildir. Biraz alışkanlık, biraz dikkat, biraz da sağlıklı şüphe ister. Telefonun ayarlarını bilmek kadar, kime ne söylediğini, hangi bilgiyi hangi ortamda paylaştığını ve bir yazışmanın ileride nasıl kullanılabileceğini düşünmek de önemlidir.

Diyarbakır'da dijital iletişimin yerel gerçekliği

Diyarbakır'da internet kullanımı farklı yaş gruplarında farklı biçimlerde ortaya çıkar. Gençler sosyal medya, oyun, mesajlaşma uygulamaları ve kısa video platformlarında daha yoğundur. Orta yaş grubu genellikle WhatsApp, Instagram, Facebook, e-Devlet, mobil bankacılık ve alışveriş uygulamalarını kullanır. Daha ileri yaşlardaki kişiler ise çoğu zaman aile grupları, görüntülü arama ve basit haber takibiyle sınırlı kalır. Riskler de bu kullanım biçimlerine göre değişir.

Örneğin üniversite öğrencisi için risk, sahte çekiliş bağlantıları, hesap ele geçirme girişimleri, özel fotoğraf ve mesajların izinsiz paylaşılması olabilir. Küçük işletme sahibi için sahte ödeme dekontları, taklit müşteri hesapları, kurumsal Instagram sayfasının çalınması veya kötü niyetli yorum kampanyaları öne çıkar. Aile büyükleri içinse banka dolandırıcılığı, kendini polis, savcı, banka görevlisi veya kargo çalışanı gibi tanıtan kişilerin mesajları daha ciddi bir tehlike oluşturur.

Yerel çevrelerin birbirine yakın olması da ayrı bir boyut yaratır. Bir şehirde herkes birbirini tanımaz ama Diyarbakır'da sosyal ağlar genellikle kesişir. Aynı okul, aynı semt, aynı akraba çevresi, aynı iş kolu veya ortak tanıdıklar üzerinden bilgiler hızla yayılabilir. Bu nedenle dijital mahremiyet yalnızca bireysel güvenlik meselesi değildir; itibar, aile ilişkileri, iş bağlantıları ve sosyal huzurla da ilgilidir.

Telefon güvenliği, işin başladığı yer

Dijital iletişimin merkezi çoğu kişi için telefondur. Telefon aynı anda kimlik cüzdanı, banka şubesi, fotoğraf albümü, sohbet arşivi, adres defteri ve iş takip aracıdır. Bu kadar çok işlevi olan bir cihazın kilitsiz bırakılması, evin kapısını açık bırakmaktan farklı değildir.

Basit ekran kilidi hâlâ en etkili savunmalardan biridir. Dört haneli kolay tahmin edilen şifreler, özellikle doğum yılı, plaka kodu, ardışık rakamlar veya tekrar eden sayılar, güvenlik hissi verse de zayıftır. Altı haneli güçlü bir PIN, parmak izi veya yüz tanıma ile birlikte kullanıldığında günlük hayatta yeterli koruma sağlar. Ancak burada küçük bir ayrıntı önemlidir: Biyometrik kilitler pratik olsa da telefon yeniden başlatıldığında, bazı güvenlik değişikliklerinde veya belirli durumlarda PIN istenir. Bu yüzden PIN kodunun hem unutulmayacak hem de tahmin edilemeyecek biçimde seçilmesi gerekir.

Telefonun işletim sistemi güncellemelerini ertelemek yaygın bir alışkanlıktır. “Sonra yaparım” denir, bildirim kapatılır ve aylar geçer. Oysa güvenlik güncellemeleri çoğu zaman görünmeyen açıkları kapatır. Güncelleme sonrasında arayüz değişebilir, bazı uygulamalar kısa süre uyumsuzluk yaşayabilir, bu doğrudur. Fakat özellikle eski Android telefonlarda güncelleme almayan cihazların risk seviyesi zamanla artar. Cihaz çok eskiyse ve artık güvenlik güncellemesi almıyorsa, bankacılık ve hassas iletişim için daha güncel bir cihaz kullanmak akıllıca olur.

Telefonu başkasına verirken de dikkat gerekir. Bir arkadaşınıza fotoğraf göstermek, çocuğa oyun açmak veya tamirciye cihaz teslim etmek normaldir, fakat bu sırada mesaj bildirimleri, galeri, notlar ve kayıtlı şifreler erişilebilir durumda olabilir. Bazı telefonlarda “uygulama sabitleme”, “misafir modu” veya “güvenli klasör” gibi seçenekler bulunur. Bu özellikler birkaç dakikalık ayarla gereksiz riskleri azaltır.

Mesajlaşma uygulamalarında mahremiyet

WhatsApp, Telegram, Signal, Instagram DM ve benzeri uygulamalar Diyarbakır’daki günlük iletişimin bel kemiği haline geldi. Aile grupları, apartman grupları, okul veli grupları, iş yeri grupları ve arkadaş çevreleri bu uygulamalarda toplanıyor. Sorun genellikle uygulamanın kendisinden değil, kullanıcı alışkanlıklarından kaynaklanıyor.

Bir mesajı göndermeden önce iki saniye beklemek basit ama güçlü bir kuraldır. Yanlış gruba atılan bir ses kaydı veya ekran görüntüsü geri alınsa bile çoktan görülmüş olabilir. Bazı uygulamalarda mesaj silme özelliği vardır, fakat bu özellik kesin güvence sağlamaz. Karşı taraf ekran görüntüsü alabilir, başka cihaza kaydedebilir veya bildirimi kilit ekranında görmüş olabilir.

Sesli mesajlar da ayrıca düşünülmelidir. Diyarbakır’da özellikle yoğun iş temposunda, araçta, çarşıda veya ev işleri sırasında sesli mesaj pratik gelir. Fakat sesli mesaj, yazılı mesaja göre daha fazla kişisel iz taşır. Arka plandaki konuşmalar, bulunduğunuz yerin sesi, yanınızdaki kişilerin adı veya özel bilgiler fark etmeden kayda girebilir. Resmi, hassas veya özel konularda sesli mesaj yerine kısa ve kontrollü yazı daha güvenli olabilir.

Grup sohbetleri ayrı bir risk alanıdır. Bir aile grubuna yeni eklenen kişi önceki mesajları göremeyebilir, fakat grupta bundan sonra yazılan her şeyi görür. İş yeri gruplarında işten ayrılan kişilerin grupta kalması, okul veli gruplarında eski numaraların unutulması, apartman gruplarında kiracı değişikliklerinin takip edilmemesi sık görülür. Grup yöneticilerinin belli aralıklarla üyeleri kontrol etmesi, özellikle telefon numarası değişikliklerinde ve görev değişimlerinde önemlidir.

Herkese açık Wi-Fi ağları ve görünmeyen riskler

Kafelerde, otogarda, hastanelerde, alışveriş noktalarında ve bazı kamu alanlarında ücretsiz Wi-Fi bulmak kolaylaştı. Bağlanması pratik, özellikle mobil veri paketi sınırlı olanlar için cazip. Fakat herkese açık Wi-Fi ağlarında iletişimin kimler tarafından izlenebileceği her zaman net değildir.

Güvenli olmayan ağlarda, özellikle şifresiz veya ortak şifreli bağlantılarda, kötü niyetli kişiler aynı ağ üzerindeki trafiği incelemeye çalışabilir. Modern bankacılık ve büyük platformlar genellikle güçlü şifreleme kullanır, bu iyi bir haberdir. Yine de sahte Wi-Fi ağına bağlanma, yanıltıcı giriş sayfasına bilgi yazma veya güvenli olmayan sitelerde oturum açma gibi riskler devam eder. Örneğin "Cafe *Free*Wifi" adıyla görünen ağ gerçekten kafenin ağı mı, yoksa yan masadaki birinin kurduğu sahte erişim noktası mı, bunu her zaman anlayamazsınız.

Hassas işlemleri mobil veriyle yapmak daha güvenlidir. Banka uygulaması, e-Devlet, iş e-postası, kimlik bilgisi içeren formlar ve özel yazışmalar için mobil veri tercih edilmelidir. Eğer herkese açık Wi-Fi kullanmak zorundaysanız, telefonun otomatik bağlanma ayarlarını kapatmak, ağ adını personelden doğrulamak ve işlem bittikten sonra ağı unutmak iyi bir alışkanlıktır.

VPN kullanımı da gündeme gelir. Güvenilir bir VPN, özellikle ortak ağlarda ek koruma sağlayabilir. Ancak her VPN güvenli değildir. Ücretsiz ve kaynağı belirsiz VPN uygulamaları, trafiğinizi korumak yerine verilerinizi toplayabilir. Bu yüzden VPN seçerken bilinen, şeffaf gizlilik politikasına sahip ve mümkünse ücretli hizmetleri tercih etmek gerekir. Yine de VPN kullanmak, sahte bağlantılara tıklamayı veya şifrenizi yanlış yere yazmayı güvenli hale getirmez.

Şifreler, iki aşamalı doğrulama ve hesap kurtarma

Birçok kişi aynı şifreyi yıllarca kullanır. E-posta, sosyal medya, alışveriş sitesi ve forum hesabı aynı şifreyle açılır. Bu pratik görünür, fakat bir sitede veri sızıntısı olduğunda diğer hesaplar da tehlikeye girer. Saldırganlar sızan e-posta ve şifre kombinasyonlarını otomatik araçlarla farklı platformlarda dener. Buna "credential stuffing" denir ve sıradan kullanıcıların hesapları çoğu zaman bu yolla ele geçirilir.

Güçlü şifre, karmaşık olmak zorunda değildir; uzun ve tahmin edilmesi zor olmalıdır. Rastgele kelimelerden oluşan uzun bir parola, kısa ama sembollerle dolu bir şifreden daha kullanışlı olabilir. Örneğin kişisel bilgi içermeyen dört veya beş kelimelik bir parola, hem yazması kolay hem de tahmin edilmesi güç olabilir. Burada önemli olan, bu kelimelerin doğum yeri, çocuk adı, takım adı, mahalle adı gibi kolay tahmin edilebilir kişisel bağlar taşımamasıdır.

İki aşamalı doğrulama artık lüks değil, temel güvenlik önlemidir. SMS ile gelen kodlar hiç yoktan iyidir, fakat SIM kart kopyalama veya hat taşıma dolandırıcılıklarında riskli olabilir. Kimlik doğrulama uygulamaları daha güvenlidir. E-posta hesabı, sosyal medya hesapları, bulut depolama ve bankacılıkla bağlantılı tüm hesaplarda iki aşamalı doğrulama açılmalıdır.

Aşağıdaki kısa kontrol, hesap güvenliğini hızlıca gözden geçirmek için kullanılabilir:

1. E-posta hesabınızın şifresi diğer tüm hesaplardan farklı olsun.
2. Ana sosyal medya hesaplarınızda iki aşamalı doğrulama açık olsun.
3. Kurtarma e-posta adresi ve telefon numarası güncel kalsın.
4. Eski, kullanılmayan uygulama bağlantılarını hesap ayarlarından kaldırın.
5. Şifrelerinizi tarayıcıya rastgele kaydetmek yerine güvenilir bir şifre yöneticisi kullanmayı değerlendirin.

Bu liste basit görünür, fakat sahada karşılaşılan hesap ele geçirme olaylarının önemli kısmı bu beş maddeden birinin eksik olmasından kaynaklanır. Özellikle e-posta hesabı kritik önemdedir. Çünkü diğer platformların şifre sıfırlama bağlantıları çoğu zaman e-postaya gelir. E-posta ele geçirilirse, domino etkisiyle birçok hesap kaybedilebilir.

Sosyal medyada görünürlük ayarları

Instagram, Facebook, TikTok, X ve benzeri platformlarda güvenli iletişim yalnızca mesajlarla sınırlı değildir. Profiliniz, paylaşımlarınız, etiketleriniz, takipçi listeniz ve konum bilgileriniz de bir iletişim biçimidir. İnsanlar hakkınızda sizin doğrudan söylemediğiniz birçok şeyi bu izlerden çıkarabilir.

Diyarbakır'da bir mekândan anlık konum paylaşmak, özellikle düzenli rutinleriniz varsa risk yaratabilir. Her cuma aynı kafede olduğunuzu, her sabah aynı güzergahtan geçtiğinizi veya evin boş kaldığı saatleri fark ettirmeden duyurabilirsiniz. Tatil fotoğraflarını anlık paylaşmak da evin boş olduğu bilgisini verebilir. Bunun yerine paylaşımları gecikmeli yapmak daha güvenlidir.

Profil gizliliği ayarları düzenli kontrol edilmelidir. Platformlar zaman zaman ayar yerlerini değiştirir, yeni özellikler ekler veya varsayılan görünürlük seçeneklerini farklılaştırır. Sadece "hesabım gizli" demek yeterli değildir. Hikâyeleri kimlerin görebildiği, etiket onayı, yorum izinleri, mesaj istekleri, telefon numarasıyla bulunabilirlik ve ortak arkadaş görünürlüğü ayrı ayrı ele alınmalıdır.

Küçük işletmeler için sosyal medya daha karmaşıktır. Bir kafe, butik, danışmanlık ofisi veya hizmet sağlayıcısı görünür olmak zorundadır. Ancak işletme hesabında kişisel telefon numarası, ev adresi, çalışanların özel bilgileri veya müşterilerin izinsiz görüntüleri paylaşılmamalıdır. Müşteri mesajları da özel veri içerir. Bir dekont ekran görüntüsü paylaşılırken IBAN, telefon, adres veya sipariş notu görünebilir. Bu tür küçük hatalar hem güven kaybına hem de hukuki sorunlara yol açabilir.

Dolandırıcılık mesajlarını tanıma

Dijital dolandırıcılıkların çoğu teknik açıdan çok gelişmiş değildir. Başarılarını insan psikolojisine borçludurlar. Acele ettirirler, korkuturlar, ödül vadederler, otorite taklidi yaparlar veya mahcubiyet yaratırlar. "Hemen ödeme yapmazsanız icra başlar", "kargonuz beklemede", "hesabınız askıya alınacak", "ödül kazandınız", "yanlışlıkla size kod geldi, iletir misiniz" gibi cümleler bu yüzden etkilidir.

Diyarbakır'da https://sites.google.com/view/diyarbakirofisescortlarihakk/ana-sayfa da sık rastlanan senaryolardan biri sahte kargo mesajıdır. Kişi zaten bir ürün bekliyordur, mesajdaki bağlantıya tıklar, küçük bir ücret ödemesi istenir, kart bilgilerini girer. Bazen ilk çekim küçük görünür, ardından daha büyük tutarlar denenir. Bir diğer örnek, sosyal medya hesabı ele **diyarbakır eskort** geçirilmiş bir tanıdıktan gelen para talebidir. Tanıdığınızın fotoğrafı ve adı kullanıldığı için güven duyarsınız, oysa hesabı başka biri yönetiyordur.

Kural şudur: Bir mesaj sizden para, şifre, doğrulama kodu veya kimlik bilgisi istiyorsa, iletişim kanalını değiştirerek doğrulayın. Banka mesajıysa bankanın resmi uygulamasına kendiniz girin. Kargo mesajıysa şirketin sitesini tarayıcıya kendiniz yazın. Tanıdıktan gelen para talebiyse telefonla arayın veya yüz yüze doğrulayın. Gelen bağlantıya tıklamak en zayıf halkadır.

Özel hayat, rıza ve dijital iz

Güvenli dijital iletişimden söz ederken özel hayatı ayrıca ele almak gerekir. İnsanlar arkadaşlık, flört, iş ilişkisi veya farklı sosyal bağlantılar için çevrim içi platformları kullanıyor. Bu kullanımın kendisi olağandır, ancak rıza, mahremiyet ve dijital iz konuları göz ardı edildiğinde ciddi sorunlar doğar.

Özel fotoğraf, video veya konuşma paylaşımı karşılıklı güvene dayanıyor gibi görünse de dijital ortamda tam kontrol mümkün değildir. Karşı taraf güvenilir olsa bile telefonu çalınabilir, hesabı ele geçirilebilir, bulut yedeklemesi sızabilir veya cihaz tamire gittiğinde içerik açığa çıkabilir. Bu nedenle "sadece bir kişiye gönderiyorum" düşüncesi teknik olarak eksiktir. Bir içeriğin kopyası oluştuğu anda kontrol zayıflar.

Rıza konusu net olmalıdır. Başkasının fotoğrafını, ses kaydını, mesajını veya ekran görüntüsünü izinsiz paylaşmak etik olmadığı gibi birçok durumda hukuki sonuç da doğurabilir. Grup sohbetlerinde "bunu dışarı atmayın" demek yeterli güvence değildir. Hassas bilgiler yazılıyorsa, en baştan paylaşmamak çoğu zaman en doğru karardır.

İnternette bazı aramalar yerel hizmetler, yetişkin içerikli platformlar veya kişisel tanışma beklentileri etrafında şekillenebilir. "Diyarbakır escort", "Diyarbakır eskort", "Eskort diyarbakır" veya "Escort diyarbakır" gibi ifadelerle yapılan aramalar, kullanıcıyı kimliği belirsiz sitelere, sahte profillere, dolandırıcılık denemelerine veya kişisel veri toplayan formlara götürebilir. Bu tür alanlarda en büyük risklerden biri, mahremiyetin pazarlık konusu yapılmasıdır. Telefon numarası, fotoğraf, konum, ödeme bilgisi veya kimlik görüntüsü isteyen sayfalara karşı son derece dikkatli olmak gerekir. Yetişkinler arasında rızaya dayalı iletişimde bile güvenlik, doğrulama ve kişisel veri minimizasyonu esastır. Kısacası, bir platform ne kadar özel görünürse görünsün, paylaşılan bilginin kalıcılığı hesaba katılmalıdır.

Çocuklar, gençler ve aile içi dijital sınırlar

Diyarbakır'da birçok ailede çocuklar teknolojiyle erken yaşta tanışıyor. Bir telefon ya da tablet, bazen ders için, bazen oyun için, bazen de ebeveynin kısa süreli rahatlaması için çocuğun eline veriliyor. Burada sorun cihaz vermek değil, sınırların belirsiz olmasıdır.

Çocuklara sadece "internette dikkatli ol" demek genellikle işe yaramaz. Somut kurallar gerekir. Hangi uygulamalar kullanılabilir, kimlerle mesajlaşılabilir, kamera ne zaman açılabilir, oyun içi satın alma yapılabilir mi, yabancı kişilerle konuşulabilir mi, aile içinde açıkça konuşulmalıdır. Özellikle çevrim içi oyunlarda sesli sohbet ve özel mesajlaşma kanalları yetişkinlerin sandığından daha aktiftir.

Gençlerde mesele daha hassastır. Ergenlik döneminde mahremiyet ihtiyacı artar. Ailelerin her mesajı okumaya çalışması güven ilişkisini zedeleyebilir. Diğer yandan tamamen kontrolsüz bırakmak da risklidir. Dengeli yaklaşım, takipten çok rehberlik üzerine kurulmalıdır. Genç bir kişi, tehdit, şantaj, ısrarlı takip veya uygunsuz mesajla karşılaştığında ailesine gidebileceğini bilmelidir. "Neden konuştun?", "Niye fotoğraf attın?", "Telefonunu alırım" gibi tepkiler, çocuğun bir sonraki sorunu saklamasına yol açabilir.

Aile içi dijital güvenlikte örnek olmak da önemlidir. Ebeveyn sürekli bilinmeyen bağlantılara tıklıyor, aile grubunda doğrulanmamış haberleri paylaşıyor, çocuğun fotoğrafını her yerde yayımlıyor veya telefon şifresini herkesin yanında söylüyorsa, çocuktan yüksek dijital farkındalık beklemek gerçekçi değildir.

İşletmeler ve serbest çalışanlar için iletişim güvenliği

Diyarbakır'da küçük işletmelerin önemli kısmı müşterileriyle doğrudan mesajlaşma üzerinden çalışıyor. Kuaför randevusu, butik siparişi, araç alım satımı, emlak görüşmesi, özel ders, tamirat, danışmanlık ve restoran rezervasyonu çoğu zaman Instagram DM ya da WhatsApp ile yürütülüyor. Bu pratiklik işletmeye hız kazandırır, fakat sınır çizilmezse karmaşa yaratır.

İşletme hesabı ile kişisel hesabı ayırmak ilk adımdır. Kişisel WhatsApp numarası üzerinden hem aile hem müşteri hem tedarikçi yazışması yapmak kısa vadede kolaydır, uzun vadede risklidir. Yanlış kişiye fiyat listesi, özel mesaj, müşteri bilgisi veya aile fotoğrafı gönderilebilir. Mümkünse ayrı bir iş hattı, işletme profili ve kurumsal e-posta kullanılmalıdır.

Müşteri verisi gereğinden fazla toplanmamalıdır. Bir randevu için ad, telefon ve saat bilgisi yeterliyse açık adres, kimlik numarası veya doğum tarihi istemenin anlamı yoktur. Hizmetin doğası gereği adres gerekiyorsa, bu bilgi iş bittikten sonra gereksiz yere sohbetlerde bırakılmamalıdır. Arşiv tutmak gerekiyorsa güvenli bir yerde, erişimi sınırlı biçimde tutulmalıdır.

Sahte ödeme dekontları küçük işletmeler için ciddi bir sorundur. Ekran görüntüsüyle gönderilen dekont tek başına kanıt sayılmamalıdır. Mobil bankacılık hesabında tutarın gerçekten geçtiği görülmeden ürün teslimi veya hizmet onayı verilmemelidir. Özellikle yoğun saatlerde, kuryeler beklerken veya müşteri acele ettirirken hata yapılır. Dolandırıcılık çoğu zaman bu acele anlarını hedefler.

E-posta ve resmi yazışmalarda dikkat

E-posta, sosyal medyaya göre daha eski görünse de resmi ve ticari iletişimde hâlâ belirleyicidir. İş başvuruları, sözleşmeler, faturalar, okul yazışmaları, belediye ve kamu kurumlarıyla iletişim, çoğu zaman e-posta üzerinden yürür. Bu yüzden e-posta güvenliği ihmal edilmemelidir.

Sahte e-postalar artık yalnızca bozuk Türkçeyle gelmiyor. Daha düzgün yazılmış, logo kullanılan, gerçek kurum adlarını taklit eden mesajlar artıyor. Gönderen adresine dikkat etmek gerekir. Görünen ad "Banka Destek" olabilir, fakat asıl e-posta adresi ilgisiz bir alan adından gelmiş olabilir. Ek dosyalar da dikkat ister. Özellikle beklenmeyen fatura, ödeme talimatı, kargo belgesi veya sıkıştırılmış dosya geldiğinde, göndereni başka kanaldan doğrulamak iyi bir pratiktir.

Resmi belge gönderirken de dosya adları ve içerikleri kontrol edilmelidir. Kimlik fotokopisi, ikametgâh, diploma, sağlık raporu veya sözleşme gibi belgeler yanlış kişiye gönderildiğinde geri almak mümkün değildir. PDF dosyalarına parola koymak bazı durumlarda yararlı olabilir, ancak parolayı aynı e-postanın içinde yazmak güvenliği azaltır. Parola gerekiyorsa farklı kanaldan iletmek daha uygundur.

Kriz anında ne yapılmalı

Hesabınız ele geçirildiğinde, özel bilgileriniz yayıldığında veya dolandırıcılığa maruz kaldığınızda panik doğal bir tepkidir. Fakat ilk saatler önemlidir. Dağınık hareket etmek yerine sıralı davranmak zararı azaltır.

1. Şifreleri güvenli bir cihazdan değiştirin, özellikle e-posta hesabından başlayın.
2. Açık oturumları kapatın ve bağlı cihazları hesap ayarlarından kontrol edin.
3. Banka veya kart bilgisi riske girdiyse bankayı hemen arayın.
4. Yakın çevrenizi bilgilendirin, hesabınızdan gelen mesajlara itibar etmemelerini söyleyin.
5. Tehdit, şantaj, izinsiz paylaşım veya maddi kayıp varsa ekran görüntüsü ve kayıtları saklayıp resmi başvuru yollarını değerlendirin.

Burada en sık yapılan hata, saldırganla uzun pazarlığa girmektir. Özellikle özel içerik tehdidiyle para isteyen kişiler, ödeme yapıldığında duracaklarının garantisini vermez. Aksine, ödeme yaptığınızı görürlerse daha fazla isteyebilirler. Böyle durumlarda kanıtları silmeden saklamak, güvendiğiniz birinden destek almak ve hukuki süreçleri düşünmek daha sağlıklı olur.

Dijital hijyen, günlük alışkanlık meselesi

Güvenlik tek seferlik bir ayar değildir. Telefonu aldığınız gün yapılan birkaç işlem yıllarca yeterli olmaz. Uygulamalar değişir, platformlar yeni özellikler ekler, dolandırıcılar farklı yöntemler dener, sosyal çevreniz genişler veya daralır. Bu yüzden dijital hijyen düzenli bakım ister.

Ayda bir kez telefonunuzdaki uygulamaları gözden geçirmek iyi bir başlangıçtır. Kullanmadığınız uygulamaları silmek, izinleri kontrol etmek, galeri ve indirilenler klasörünü temizlemek, eski ekran görüntülerini ayıklamak hem güvenlik hem de düzen sağlar. Uygulamaların kamera, mikrofon, konum ve rehber erişimleri özellikle

incelenmelidir. Bir el feneri uygulamasının rehbere erişmek istemesi makul değildir. Bir alışveriş uygulamasının sürekli konum takibi yapması her zaman gerekli olmayabilir.

Bildirim ayarları da mahremiyetin parçasıdır. Kilit ekranında mesaj içeriğinin görünmesi, telefon masadayken yanınızdaki herkesin özel konuşmaları okumasına neden olabilir. İçerik gizleme ayarı küçük ama etkili bir çözümdür. Özellikle iş yerinde, okulda, kafede veya toplu taşıma sırasında telefon ekranı fark edilmeden okunabilir.

Bulut yedeklemeleri unutulmamalıdır. Fotoğraflarınız, mesajlarınız ve belgeleriniz otomatik olarak buluta yedekleniyor olabilir. Bu pratik bir korumadır, telefon kaybolduğunda veriyi kurtarır. Fakat bulut hesabınız zayıf şifreyle korunuyorsa risk artar. Bulut yedeklerini kapatmak yerine, hesabı güçlü şifre ve iki aşamalı doğrulamayla korumak daha dengeli bir çözümdür.

Güven ile şüphe arasındaki denge

Dijital iletişimde aşırı korku da sağlıklı değildir. Her mesajdan şüphe etmek, hiçbir platforma güvenmemek, sürekli takip edildiğini düşünmek insanı yorar ve iletişimi verimsiz hale getirir. Ama sınırsız güven de sorunludur. Doğru yaklaşım, makul şüphe ve iyi alışkanlık dengesidir.

Tanıdığınız kişilere güvenebilirsiniz, fakat hesaplarının ele geçirilebileceğini unutmayın. Bilinen markalardan gelen mesajları dikkate alabilirsiniz, fakat bağlantıya tıklamadan önce adresi kontrol edin. Ücretsiz Wi-Fi kullanabilirsiniz, fakat bankacılık işlemini mobil veriyle yapın. Sosyal medya paylaşımı yapabilirsiniz, fakat anlık konum ve özel bilgileri sınırlayın. Bu tür küçük kararlar bir araya geldiğinde güçlü bir güvenlik kültürü oluşturur.

Diyarbakır'ın sosyal yapısı, dayanışmayı kolaylaştırır. Bir dolandırıcılık mesajı aile grubunda hızla duyurulabilir, yaşlı bir akrabanın telefon ayarları birlikte kontrol edilebilir, küçük bir işletme komşu esnafı sahte dekont konusunda uyarabilir. Aynı sosyal yapı, dikkatsiz paylaşımda bilginin hızla yayılmasına da neden olur. Bu yüzden teknolojiyle birlikte sosyal sorumluluk da gerekir.

Güvenli dijital iletişim, uzmanlara bırakılacak kadar uzak bir konu değildir. Herkesin öğrenebileceği, uygulayabileceği ve çevresine aktarabileceği pratiklerden oluşur. Güçlü şifre, dikkatli bağlantı kontrolü, sınırlı paylaşım, güncel cihaz, doğrulanmış iletişim kanalı ve rızaya saygı, temel taşları oluşturur. Diyarbakır'da dijital hayat büyüdükçe, bu temel taşların değeri daha da artacaktır. Ekran üzerinden kurulan her iletişim, gerçek hayatta bir karşılık bulur; bu yüzden güvenliği de gerçek hayat ciddiyetiyle ele almak gerekir.