Diyarbakır'da çevrim içi dolandırıcılık denince çoğu kişinin aklına hâlâ "bana denk gelmez" düşüncesi gelir. Oysa dolandırıcılık artık yalnızca teknolojiye uzak kişileri hedef alan basit mesajlardan ibaret değil. Banka müşterisi olan, ikinci el eşya satan, kargo bekleyen, sosyal medyada alışveriş yapan, iş arayan, ilan sitelerine bakan, hatta sadece bir bağlantıya tıklayan herkes risk alanına giriyor. Kentin günlük hayatı dijitalleştikçe, dolandırıcıların kullandığı yöntemler de yerelleşiyor. Diyarbakır adının, semtlerin, yerel işletmelerin, kargo şubelerinin, kamu kurumlarının ya da tanıdık kültürel ifadelerin kullanıldığı sahte mesajlar daha inandırıcı görünebiliyor.

Bu konuda en kritik nokta, dolandırıcılığı yalnızca "teknik" bir sorun gibi görmemek. Evet, güçlü şifre, iki aşamalı doğrulama, güvenli bağlantı önemlidir. Fakat dolandırıcılığın merkezinde çoğu zaman insan davranışı vardır. Acele ettirme, utandırma, merak uyandırma, fırsatı kaçırma korkusu yaratma, resmi görünme, mahremiyet baskısı kurma gibi taktikler, teknik açıklardan daha etkili olabiliyor. Diyarbakır'da yaşayan biri için bu riskler bazen bir banka mesajında, bazen bir emlak ilanında, bazen de sosyal medya üzerinden gelen tanıdık görünümlü bir hesapta ortaya çıkıyor.

Diyarbakır'da çevrim içi dolandırıcılık neden daha görünür hale geldi?

Diyarbakır, genç nüfusu, yoğun ticari hareketliliği, üniversite çevresi, ilçeler arası canlı alışveriş ilişkileri ve sosyal medya kullanımının yaygınlığı nedeniyle dijital dolandırıcılar için geniş bir hedef alanı sunuyor. Bu, kente özgü bir kusur değil. İstanbul, Ankara, İzmir, Gaziantep, Şanlıurfa ve diğer büyük şehirlerde de benzer tablo var. Fark şu ki, dolandırıcılar artık genel mesajlar yerine yerel detaylarla güven kazanmaya çalışıyor.

Örneğin "Diyarbakır içi aynı gün teslim", "Bağlar'da elden ödeme", "Kayapınar'da acil satılık", "Sur civarı iş ilanı", "Yenişehir şubesinden arıyoruz" gibi ifadeler, alıcının dikkatini düşürebiliyor. Kişi, mesajın yerel bir bağ taşıdığını görünce kaynağı daha az sorgulayabiliyor. Oysa dolandırıcılar bu tür ifadeleri sosyal medya ilanlarından, harita yorumlarından, açık profil bilgilerinden veya rastgele tahminlerden kolayca derleyebiliyor.

Bir başka neden de dijital ödeme alışkanlıklarının hızla yayılması. Havale, FAST, sanal kart, QR ödeme ve mobil bankacılık gündelik hale geldi. Bu kolaylık, doğru kullanıldığında hayatı hızlandırır. Fakat aynı hız, yanlış bir IBAN'a para gönderildiğinde veya sahte bir ödeme ekranına kart bilgisi girildiğinde geri dönüşü zorlaştırabilir. Bankalar belirli durumlarda işlem takibi yapabilir, ama dolandırıcılıkta zaman kaybı çoğu zaman zararı büyütür.

En sık karşılaşılan yöntemler: basit görünen ama etkili tuzaklar

Diyarbakır'da da Türkiye'nin genelinde olduğu gibi en yaygın çevrim içi dolandırıcılık türlerinin başında sahte banka ve kargo mesajları geliyor. "Hesabınız askıya alındı", "Kartınız güvenlik nedeniyle kapatılacak", "Kargonuz teslim edilemedi", "Adres güncellemesi gerekli" gibi ifadelerle gelen SMS veya e-posta mesajları, kullanıcıyı sahte bir bağlantıya yönlendiriyor. Bağlantı açıldığında gerçek bankaya ya da kargo şirketine benzeyen bir sayfa çıkıyor. Logo doğru görünebilir, renkler aynı olabilir, hatta sayfa mobilde oldukça profesyonel durabilir. Tehlike de burada başlar. Kullanıcı kart numarası, şifre, SMS kodu veya kimlik bilgisi girdiğinde bilgiler dolandırıcının eline geçer.

Sosyal medya üzerinden yapılan alışveriş dolandırıcılıkları da sık görülüyor. Özellikle elektronik eşya, telefon, küçük ev aleti, uygun fiyatlı mobilya, araç parçası, bebek ürünü, yöresel ürün ve bilet satışı gibi alanlarda sahte hesaplar açılıyor. Hesapta eski tarihli gönderiler, yorumlar ve takipçi sayısı olabilir. Fakat bunların bir kısmı satın alınmış ya da kopyalanmış olabilir. Dolandırıcı genellikle "kapora gönder", "ürünü ayırayım", "kargo çıkışı için ödeme alayım" gibi cümlelerle küçük bir miktar ister. İlk miktar düşük olduğunda kişi daha kolay ödeme yapar. Ardından ikinci ödeme, sigorta bedeli, kargo farkı veya iptal ücreti gibi yeni bahaneler gelir.

İlan sitelerinde de benzer yöntemler kullanılır. Kiralık ev, araç, iş ilanı, ikinci el ürün veya hizmet ilanlarında “çok uygun fiyat” en belirgin işarettir. Diyarbakır’da özellikle üniversite öğrencilerinin ve şehir dışından gelenlerin ev aradığı dönemlerde sahte kiralık ev ilanları artabilir. Fotoğraflar gerçek bir evden alınmıştır, adres merkezi görünür, kira piyasanın altındadır. Arayan kişiye “çok talep var, evi kaçırmamak için depozito gönderin” denir. Evi görmeden para göndermek, bu senaryoda en büyük risktir.

Bazı dolandırıcılıklar ise mahremiyet ve utanç duygusu üzerinden yürür. Kullanıcıların arama motorlarında veya sosyal medya platformlarında yazdığı hassas kelimeler, sahte siteler için yem olarak kullanılır. Örneğin “Diyarbakır escort”, “Diyarbakır eskort”, “Eskort diyarbakır” veya “Escort diyarbakır” gibi aramalar üzerinden kurulan sahte sayfalar, kişileri kapora, kimlik fotoğrafı, özel görüntü tehdidi veya şantajla hedef alabilir. Burada konu yalnızca yasa dışı ya da riskli içeriklere erişim değildir. Dolandırıcı, kişinin çekinerek yardım istemesini kullanır. Mağdur, utanacağı düşüncesiyle bankasına, ailesine ya da kolluk birimlerine başvurmakta geç kalabilir. Bu gecikme dolandırıcının lehine işler.

Dolandırıcıların kullandığı psikolojik baskı

Teknik güvenlik önlemleri elbette gerekir, fakat dolandırıcının asıl silahı çoğu zaman duygudur. Bir mesaj sizi paniklettiğinde, normalde yapmayacağınız bir şeyi birkaç dakika içinde yapabilirsiniz. “Hesabınızdan para çekiliyor”, “Savcılık dosyanız var”, “Kargonuz iade olacak”, “Son 10 dakika”, “Hemen ödeme yapmazsanız işlem iptal olur” gibi cümleler, kişinin düşünme süresini kısaltmak için tasarlanır.

Diyarbakır’da küçük esnafla konuştuğunuzda benzer hikâyeler duyarsınız. Bir işletme hesabına gelen sahte reklam mesajı, bir kargo linki, bir tedarikçi ödemesi, bir müşteriden gelmiş gibi görünen dekont görüntüsü. Bazı dolandırıcılar işletmenin sosyal medya hesabını ele geçirmeye çalışır. Hesap ele geçirildiğinde yalnızca işletme zarar görmez, o hesabı takip eden müşteriler de sahte kampanyalarla hedef alınır. “Bugüne özel çekiliş”, “hediye kazandınız”, “kargo ücretini yatırın” gibi mesajlar, tanıdık bir işletme hesabından gelince daha inandırıcı olur.

Aynı baskı bireysel ilişkilerde de görülür. Dolandırıcı, kendini asker arkadaşı, eski okul tanıdığı, uzaktan akraba, kurye, banka görevlisi, polis, avukat veya savcı olarak tanıtabilir. Gerçek kurum çalışanları telefonla sizden şifre, kart numarası, mobil bankacılık onay kodu istemez. Bu cümle basit görünür ama pratikte çok hayat kurtarır. Çünkü dolandırıcıların çoğu, “zaten biliyordum ama o an panikledim” dedirtecek kadar iyi rol yapar.

Güvenli davranışın temel ilkeleri

Çevrim içi dolandırıcılığa karşı korunmada karmaşık terimlere boğulmaya gerek yok. Esas olan, para, kimlik ve hesap erişimiyle ilgili her işlemde kısa bir duraksama alışkanlığı edinmektir. Özellikle mobil telefonda işlem yaparken ekran küçük olduğu için sahte adresleri fark etmek zorlaşır. Bu nedenle bağlantıya tıklamak yerine uygulamayı kendiniz açmak daha güvenlidir. Banka işlemi gerekiyorsa bankanın resmi uygulamasını açın. Kargo sorgulaması gerekiyorsa firmanın resmi web sitesine adresi kendiniz yazarak girin. E-devlet işlemi için arama motorundan çıkan reklamlara değil, doğrudan resmi adrese güvenin.

Aşağıdaki kısa kontrol, şüpheli bir mesaj aldığınızda çoğu tuzağı elemenize yardımcı olur:

1. Mesaj sizi aceleye zorluyor mu, hemen ödeme veya şifre istiyor mu?
2. Bağlantı adresi resmi kurumun gerçek alan adıyla birebir aynı mı?
3. Sizden SMS kodu, kart şifresi, mobil bankacılık onayı veya kimlik fotoğrafı isteniyor mu?
4. Teklif piyasa değerine göre belirgin biçimde ucuz mu?
5. Karşı taraf görüntülü görüşmeden, yüz yüze işlemden veya resmi ödeme kanalından kaçıyor mu?

Bu sorulardan birine bile “evet” diyorsanız işlem durdurulmalı. Dolandırıcılıkta en etkili savunma bazen hiçbir şey yapmamaktır. Linke tıklamamak, ödeme göndermemek, kod paylaşmamak, konuşmayı kapatmak. Kaba olmak zorunda değilsiniz, ama kararlı olmanız gerekir. Gerçek bir kurum ya da güvenilir satıcı, sizin doğrulama yapmak istemenizden rahatsız olmaz.

Banka, kart ve ödeme güvenliği

Mobil bankacılık güvenliği, yalnızca şifreyi güçlü seçmekten ibaret değildir. Telefonunuza kurduğunuz uygulamalar, kullandığınız ekran kilidi, SIM kart güvenliği, e-posta hesabınız ve hatta sosyal medya hesaplarınız bankacılık güvenliğini etkiler. Çünkü birçok hesap kurtarma işlemi telefon numarası veya e-posta üzerinden yapılır. E-posta hesabınız ele geçirilirse, dolandırıcı diğer hesaplarınıza da erişmeye çalışabilir.

Şifrelerde yapılan en yaygın hata, aynı şifreyi birçok yerde kullanmaktır. Bir alışveriş sitesinden sızan şifre, başka bir platformda denenebilir. Buna “credential stuffing” denir, teknik adı karmaşık olsa da mantığı basittir. Dolandırıcı, sizin bir yerde kullandığınız e-posta ve şifreyi başka yerlerde de dener. Bu yüzden banka, e-posta ve sosyal medya hesaplarında benzersiz şifre kullanmak gerekir. Şifre yöneticileri bu noktada işe yarar, fakat herkes kullanmak istemeyebilir. Kullanmayacaksanız bile en azından kritik hesaplarda birbirinden tamamen farklı şifreler seçin.

Kart güvenliğinde sanal kart iyi bir ara çözümdür. İnternetten alışveriş yaparken limiti düşük bir sanal kart kullanmak, kart bilgilerinizin kötüye kullanılması halinde zararı sınırlar. Ancak sanal kart da tek başına yeterli değildir. Sahte ödeme sayfasına SMS onay kodu girerseniz, limit dahilinde işlem yapılabilir. Bu nedenle bankadan gelen SMS veya uygulama bildirimlerini okumadan onaylamayın. Bildirimde tutar, iş yeri adı ve işlem türü yazar. “Zaten ben işlem yapıyorum” diyerek otomatik onay vermek, dolandırıcının beklediği davranıştır.

FAST ve havale işlemlerinde de alıcı adı kontrolü önemlidir. IBAN’a para gönderirken bankanın gösterdiği alıcı adıyla işlem yaptığınız kişi aynı mı bakın. “Şirket hesabı kapalı, kuzenimin IBAN’ına gönderin”, “muhasebecinin hesabı”, “kargo firmasının hesabı” gibi açıklamalar risklidir. Bireysel hesaba yapılan ödemelerde iade süreci daha zor olabilir. Özellikle kapora ve ön ödeme taleplerinde, karşı tarafın kimliği ve hizmetin gerçekliği doğrulanmadan para gönderilmemelidir.

Sosyal medya hesaplarını korumak

Sosyal medya hesapları artık yalnızca fotoğraf paylaşılan alanlar değil. Küçük işletmeler sipariş alıyor, gençler iş buluyor, aileler haberleşiyor, esnaf müşteriyle iletişim kuruyor. Bir hesabın ele geçirilmesi, maddi zararın yanında itibar kaybı da yaratır. Diyarbakır’da bir kafe, butik, kuaför, oto galeri veya yöresel ürün satıcısının hesabı çalındığında, takipçilere gönderilen sahte kampanya mesajları kısa sürede yayılabilir. İnsanlar tanıdıkları işletmeye güvendikleri için ödeme yapabilir.

Hesap güvenliği için iki aşamalı doğrulama mutlaka açılmalı. Mümkünse SMS yerine doğrulama uygulaması tercih edilmeli, çünkü SIM kart kopyalama veya numara taşıma saldırıları nadir de olsa ciddi sonuç doğurabilir. Kurtarma e-postası güncel olmalı. Hesaba bağlı telefon numarası size ait olmalı. Tanımadığınız cihazlardan giriş uyarılarını dikkate alın. Bir bağlantı “mavi tik başvurusu”, “telif ihlali”, “hesabınız kapanacak”, “reklam borcunuz var” gibi gerekçelerle şifre istiyorsa büyük ihtimalle sahtedir.

İşletme hesaplarında yetki paylaşımı ayrıca önemlidir. Hesabın şifresini herkesin bilmesi pratik görünebilir, fakat risklidir. Mümkün olan platformlarda kişi bazlı yönetici yetkisi verilmeli, işten ayrılan kişilerin erişimi kaldırılmalı, şifreler düzenli olarak değiştirilmelidir. Bir işletmede sosyal medya hesabına hem kasadaki telefon, hem evdeki tablet, hem çalışanların kişisel cihazları bağlıysa, güvenlik zinciri en zayıf cihaz kadar güçlüdür.

Sahte ilanlar, kiralık evler ve ikinci el alışveriş

Diyarbakır'da kiralık ev arayan öğrenciler, tayinle gelen memurlar, yeni evlenecek çiftler ve ilçelerden merkeze taşınmak isteyen aileler dönem dönem yoğun bir ilan trafiğiyle karşılaşır. Dolandırıcılar bu dönemleri izler. Gerçek ev fotoğraflarını başka şehirlerden alıp Diyarbakır adresiyle yayınlayabilirler. Hatta haritada makul bir konum işaretleyip açıklamaya çevredeki bilinen yerleri ekleyebilirler. İlanın dili ne kadar ayrıntılıysa o kadar gerçek sanılabilir.

Evi görmeden depozito göndermek en büyük hatadır. "Şehir dışındayım", "anahtar emlakçıda ama çok talep var", "önce kapora atan kişiye göstereceğim" gibi bahaneler sık kullanılır. Gerçek bir kiralama işleminde ev görülür, mal sahibi veya yetkili emlakçı doğrulanır, tapu veya yetki belgesi kontrol edilir, sözleşme yapılır. Emlakçıyla çalışılıyorsa yetki ve ofis bilgileri teyit edilmelidir. Bir kişinin sadece telefonda güven vermesi yeterli değildir.

İkinci el alışverişte de benzer dikkat gerekir. Özellikle telefon, bilgisayar, oyun konsolu, beyaz eşya ve araç parçası gibi ürünlerde fiyata dikkat edin. Piyasa değeri 20 bin lira olan bir ürün 8 bin liraya satılıyorsa bunun bir nedeni vardır. Acil nakit ihtiyacı gerçek https://sites.google.com/view/diyarbakirescortrehberi/ana-sayfa olabilir, ama dolandırıcıların en sevdiği kılıf da budur. Elden alışverişte ürünü çalışır halde görmek, seri numarasını kontrol etmek, faturayı istemek ve kalabalık, güvenli bir noktada buluşmak daha sağlıklıdır. Kargo ile alışverişte güvenli ödeme sistemi sunan platformları kullanmak, doğrudan IBAN'a ödeme yapmaktan daha güvenlidir.

İş ilanları ve "kolay para" vaatleri

Çevrim içi iş dolandırıcılıkları son yıllarda belirgin şekilde arttı. Evden çalışma, paketleme işi, sosyal medya görevi, beğeni yaparak para kazanma, kripto yatırım asistanlığı, sahte çağrı merkezi, ürün yorumlama gibi başlıklarla insanlar hedef alınabiliyor. Diyarbakır'da iş arayan gençler, öğrenciler ve ek gelir isteyen aileler bu ilanlara sıkça rastlayabiliyor. İlk temas genellikle mesajlaşma uygulaması üzerinden kuruluyor. Başvuru formu adı altında kimlik bilgisi, IBAN, adres, hatta kimlik fotoğrafı istenebiliyor.

Bazı dolandırıcılıklarda mağdurdan başlangıç ücreti talep edilir. "Kayıt bedeli", "sigorta girişi", "malzeme kaporası", "eğitim ücreti" gibi adlar kullanılır. Bazılarında ise mağdurun banka hesabı para transferi için kullanılır. Bu daha tehlikelidir, çünkü kişi farkında olmadan yasa dışı para trafiğinin parçası haline gelebilir. "Hesabına para gelecek, sen komisyonunu alıp kalanını göndereceksin" gibi teklifler kesinlikle reddedilmelidir. Meşru bir işveren, çalışan adayının kişisel banka hesabını üçüncü kişilerden para toplamak için kullanmaz.

İş ilanlarında şirketin ticaret unvanı, vergi bilgisi, açık adresi, sabit telefonu, kurumsal e-posta adresi ve görüşme süreci kontrol edilmelidir. Sadece mesajlaşma uygulamasıyla yürüyen, yüz yüze ya da görüntülü görüşmeden kaçan, işi açıklamadan kimlik isteyen ilanlar risklidir. İş arayan kişinin çaresizliğini kullanmak, bu dolandırıcılık türlerinin temel taktiğidir.

Mahremiyet üzerinden şantaj ve kapora dolandırıcılığı

Çevrim içi dolandırıcılığın en az konuşulan ama en yıpratıcı türlerinden biri mahremiyet temelli şantajdır. Sahte profillerle yakınlık kurma, görüntülü konuşma kaydı tehdidi, özel fotoğraf isteme, yetişkin içerik vaadiyle kapora alma veya tanışma siteleri üzerinden para talep etme gibi yöntemler kullanılır. Bu tür olaylarda mağdurun ilk tepkisi genellikle paniktir. Dolandırıcı da tam bunu ister. "Ailene gönderirim", "iş yerine yollarım", "sosyal medyada paylaşırım" gibi tehditlerle yeni ödemeler almaya çalışır.

Bu noktada para göndermek çoğu zaman sorunu çözmez. İlk ödeme, dolandırıcıya mağdurun korktuğunu gösterir ve yeni taleplerin kapısını açar. Tehdit içeren mesajlar silinmeden saklanmalı, ekran görüntüleri alınmalı, profil bağlantıları ve ödeme bilgileri kaydedilmelidir. Ardından bankayla ve yetkili birimlerle hızlıca iletişime

geçilmelidir. Utanç duygusu anlaşılır, fakat gecikme zararı artırır. Bu tür olaylar yalnızca mağdurun "dikkatsizliği" ile açıklanamaz. Dolandırıcılar profesyonel biçimde manipülasyon yapar, sahte kimlikler kullanır ve aynı anda birçok kişiyi hedefler.

Arama motorlarında karşılaşılan bazı yetişkin içerikli veya arkadaşlık amaçlı sayfalar da benzer risk taşır. Yerel anahtar kelimeler kullanılarak açılan sahte siteler, Diyarbakır'da yaşayan kişileri hedefliyormuş gibi görünebilir. Bu sayfalarda kapora talebi, kimlik doğrulama bahanesiyle belge isteme, konum paylaşımı ve özel bilgi toplama sık görülür. Kişisel güvenlik açısından bu tür ortamlarda kimlik, adres, iş yeri, aile bilgisi, canlı konum ve banka bilgisi paylaşılmamalıdır.

Çocuklar, gençler ve aile içi dijital farkındalık

Dolandırıcılık yalnızca yetişkinlerin sorunu değildir. Çocuklar ve gençler oyun hesapları, hediye kartları, ücretsiz kostüm veya oyun parası vaatleri, sahte çekilişler ve sosyal medya hesap çalma yöntemleriyle hedef alınır. Bir çocuğun oyun hesabı ele geçirildiğinde aile bunu küçük bir kayıp gibi görebilir. Ancak aynı şifre e-posta hesabında veya başka platformlarda da kullanılıyorsa risk büyür. Ayrıca çocuklardan aile kartı bilgisi istenebilir ya da cihazlarına zararlı yazılım yükletilebilir.

Ailelerin yasaklayıcı bir dil yerine konuşmaya açık bir tutum benimsemesi daha etkili olur. Çocuk bir hata yaptığında aşırı tepki göreceğini düşünürse olayı saklar. Dolandırıcılığın erken fark edilmesi için çocuğun "yanlış bir yere tıkladım" diyebilmesi gerekir. Evde basit kurallar belirlenebilir: kart bilgisi girilmez, bilinmeyen bağlantı açılmaz, hediye kazandığını söyleyen hesaba inanılmaz, oyun içi takaslarda hesap şifresi verilmez. Bu kurallar ara sıra tekrarlandığında, kriz anında daha kolay hatırlanır.

Gençler için bir başka risk de sahte burs ve yardım başvurularıdır. Öğrencilerden kimlik, IBAN, e-devlet bilgisi veya "başvuru onayı" için ücret istenebilir. Gerçek burs veren kurumlar da belge talep edebilir, fakat başvuru adresi, kurumun resmi sitesi ve iletişim bilgileri doğrulanmalıdır. E-devlet şifresi hiçbir kurum, dernek, vakıf veya kişiyle paylaşılmamalıdır.

Dolandırıcılığa maruz kalındığında ilk saatler

Dolandırıcılık fark edildiğinde yapılacak en kötü şey donup kalmaktır. İlk saatlerde doğru adımlar atılırsa zararın büyümesi engellenebilir. Banka işlemi yapıldıysa hemen bankanın müşteri hizmetleri aranmalı, işlem bildirilmeli, kartlar geçici olarak kapatılmalı veya limitler sıfırlanmalıdır. Mobil bankacılık şifresi değiştirilmelidir. E-posta hesabı ve sosyal medya hesapları kontrol edilmelidir. Aynı şifre başka yerlerde kullanılıyorsa onlar da değiştirilmelidir.

Delil toplamak önemlidir. Mesajları, telefon numaralarını, IBAN bilgilerini, kullanıcı adlarını, ilan bağlantılarını, dekontları ve ekran görüntülerini saklayın. Dolandırıcıyla tartışmak, tehdit etmek veya uzun pazarlığa girmek genellikle fayda sağlamaz. Hatta bazı durumlarda karşı tarafın delilleri silmesine yol açabilir. Bunun yerine belgeleyip resmi başvuru yapmak daha doğru olur.

Başvuru için kolluk birimlerine veya savcılığa gidilebilir. Ayrıca ilgili platformlara şikâyet yapılmalı, sahte hesaplar bildirilmelidir. Banka kanalıyla para transferi olduysa alıcı banka bilgileri de süreçte önem taşır. Para mutlaka geri döner demek doğru olmaz, çünkü dolandırıcılar parayı hızla başka hesaplara aktarabilir. Yine de hızlı bildirim, şansı artırır ve en azından başka kişilerin zarar görmesini önlemeye katkı sağlar.

Şu kısa kriz planı pratikte işe yarar:

1. Bankayı arayın, kartları ve şüpheli işlemleri durdurun.
2. Şifreleri değiştirin, özellikle e-posta ve mobil bankacılığı güvenceye alın.
3. Delilleri silmeden ekran görüntüsü ve kayıt alın.
4. Platforma, bankaya ve yetkili birimlere resmi bildirim yapın.
5. Yakın çevrenizi uyarın, ele geçirilen hesaplardan gelen mesajlara itibar edilmemesini söyleyin.

Yerel işletmeler için ek önlemler

Diyarbakır'daki işletmeler çevrim içi görünürlüklerini artırırken güvenlik süreçlerini de işin parçası haline getirmeli. Bir işletmenin Instagram hesabı, Google işletme profili, WhatsApp hattı veya e-ticaret sayfası müşteriyle doğrudan temas noktasıdır. Bu kanallarda yaşanan bir ihlal, müşteri güvenini zedeler. Özellikle restoranlar, kafeler, butik mağazalar, güzellik salonları, telefoncular, oto galeriler, emlakçılar ve yöresel ürün satıcıları sahte hesap taklitleriyle sık karşılaşabilir.

Taklit hesaplar genellikle gerçek hesabın fotoğraflarını kopyalar, kullanıcı adına nokta veya alt çizgi ekler, takipçilere mesaj atar. "Çekiliş kazandınız", "ödül için kargo ücreti", "kampanya kaporası" gibi ifadeler kullanılır. İşletmeler resmi hesap kullanıcı adını görünür biçimde paylaşmalı, müşterilerine yalnızca belirli ödeme kanallarını kullandıklarını bildirmeli ve taklit hesapları hızlıca duyurmalıdır. Web sitesi varsa sosyal medya bağlantıları sitede yer almalı. Müşteri ödeme yapmadan önce doğru hesapla iletişimde olduğunu anlayabilmelidir.

Çalışan eğitimi de basit ama etkili bir adımdır. Kasadaki personel, sosyal medya mesajlarına bakan çalışan veya sipariş alan kişi, sahte dekontu nasıl ayırt edeceğini bilmelidir. Dekont görüntüsü tek başına ödeme kanıtı değildir. Para hesaba geçmeden ürün teslim etmek risklidir. Bazı dolandırıcılar ileri tarihli EFT dekontu, düzenlenmiş ekran görüntüsü veya iptal edilmiş işlem görüntüsü gönderir. İşletme içinde "hesapta görünmeyen ödeme için ürün çıkmaz" kuralı net olmalıdır.

Her bağlantıya değil, doğrulama alışkanlığına güvenmek

Çevrim içi güvenlikte kusursuz araç yoktur. Antivirüs programı, banka güvenlik sistemi, telefon uyarıları ve platform denetimleri riskleri azaltır, ama tamamen ortadan kaldırmaz. Kullanıcının doğrulama alışkanlığı bu yüzden belirleyicidir. Bir mesaj gerçek gibi görünüyorsa bile kaynağı ayrı bir kanaldan kontrol etmek gerekir. Bankadan arandığınızı söyleyen kişiyi dinlemek yerine telefonu kapatıp bankanın resmi numarasını kendiniz arayın. Kargo mesajındaki bağlantıya tıklamak yerine kargo firmasının sitesine kendiniz girin. Sosyal medyada tanıdığınızdan para isteyen bir mesaj geldiyse o kişiyi telefonla arayın.

Bu yaklaşım zaman kaybettiriyor gibi görünebilir. Gerçekte birkaç dakika ayırmak, günlerce sürecek bir mağduriyeti önler. Dolandırıcılar hız ister, güvenli kullanıcı yavaşlar. Bu basit fark, çoğu saldırıyı boşa çıkarır.

Diyarbakır’da çevrim içi dolandırıcılıktan korunmak için teknoloji bilgini olmak gerekmez. Dikkatli olmak, acele etmemek, ödeme öncesi doğrulamak, şifreleri korumak ve mahremiyet baskısına teslim olmamak yeterli temeli oluşturur. Kentin sosyal yapısında güven önemli bir değerdir, fakat dijital ortamda güven doğrulamayla desteklenmediğinde kolayca istismar edilir. Bir mesajın Diyarbakır’dan bahsetmesi, bir ilanın yerel görünmesi, bir hesabın tanıdık fotoğraflar kullanması veya bir kişinin resmi konuşması tek başına kanıt değildir. Kanıt, doğrulanabilir bilgi ve güvenli işlem sürecidir.

Her kullanıcı kendi çevresinde küçük bir güvenlik halkası kurabilir. Aile büyüklerine sahte banka mesajlarını anlatmak, çocuklara oyun şifresi paylaşmamayı öğretmek, işletme çalışanlarına sahte dekont riskini göstermek, arkadaşları şüpheli ilanlara karşı uyarmak bu halkanın parçalarıdır. Dolandırıcılık bireysel bir olay gibi başlar, ama etkisi aileye, işletmeye ve çevreye yayılır. Aynı şekilde bilinç de yayıldığında koruma gücü artar.