Sayın Yetkili,

Uluslararası Hava Taşımacılığı Birliği (IATA), hava taşımacılığı sektörü katılımcılarına dolandırıcılık eylemleri konusunda tetikte olmalarına yönelik yıllık hatırlatmasını yapmaktadır. Hava taşımacılığı sektörü, dolandırıcılık girişimleri için yaygın bir hedeftir. Son dolandırıcılık yöntemleri arasında, kimlik avı saldırılarında IATA personelinin kimliğine bürünme, IATA logosunu ve adını potansiyel müşterileri dolandırmak amacıyla kullanma ve yasa dışı hesaplara ödeme yönlendirme girişimleri yer almıştır. IATA, dolandırıcılık girişimlerini tespit etmenize yardımcı olacak bazı değerli bilgileri sizlerle paylaşmayı uygun görmektedir.

Aşağıdaki birkaç adım sizi "Fraudulent Emails Warning" (Dolandırıcılık Amaçlı E-posta Uyarısı) adlı gözden geçirilmiş kılavuzumuza yönlendirecektir. Bu kılavuz, dolandırıcıların kullandığı farklı tekniklere örnekler ve şirketinizi dolandırıcılığa karşı daha iyi korumak için öneriler sunmaktadır.[1]

1. IATA web sitesini ziyaret edin: www.iata.org.
2. Sayfanın üst bölümünden "Contact & Support" (İletişim ve Destek) üzerine tıklayın. Mobil bir cihaz kullanıyorsanız, bu bağlantıyı ekranınızın sağ üst köşesindeki açılır menüde bulabilirsiniz.
3. "Report a fraudulent e-mail or check the validity of an e-mail" (Dolandırıcılık amaçlı bir e-posta bildir veya bir e-postanın geçerliliğini kontrol et) adlı bağlantıya tıklayın. Bu bağlantısı sizi Email & Website Fraud Protection (E-posta ve Web Sitesi Dolandırıcılığından Korunma) web sayfasına ("Web Sayfası") yönlendirecektir.
4. Web sayfasının sağ tarafında bulunan "Related Links" (İlgili Bağlantılar) bölümünden Fraudulent e-mails warning (Dolandırıcılık amaçlı e-posta uyarısı) bağlantısına tıklayın. Mobil bir cihaz kullanıyorsanız, bu bağlantıyı sayfanın alt bölümünde bulabilirsiniz.

Önemli noktalar:

- Dolandırıcılar sahte adlar kullanarak ya da IATA çalışanlarının adlarını kullanarak IATA ürün ve hizmetlerinin kullanıcıları ile e-posta veya telefon yoluyla iletişime geçmekte ve ürün veya hizmetler için ve/veya ödenmemiş borçlar için ödeme talep etmektedir.

- Dolandırıcılar düzenli olarak her büyüklükteki birçok acente ve hava yolu ile iletişime geçmektedir.

- Dolandırıcılar bir IATA e-posta adresine benzer, "@gmail.com" veya "@iattafinance.org" gibi farklı alan adlı e-posta adresleri kullanmaktadır.

1 http://www.iata.org/Documents/Fraud-Prevention/Fraudulent-emails-warning.pdf

- Çoğu zaman e-posta hesapları maskelenmekte, böylece e-postalar “@iata.org” alan adlı gerçek bir IATA adresinden gönderilmiş gibi görünmektedir. Buna kimlik sahtekarlığı denir. Yanıt e-posta adresi genellikle farklıdır veya e-posta sizi sahte bir web sayfasına götüren bağlantıya tıklamanız için yönlendirir. Örneğin, “iata@iata.org” adresinden gelen bir e-posta, yanıtla düğmesine tıkladıktan sonra “revenue@iata-payments.org” olarak görünecektir.

- Sahte belgelerde sık sık IATA logosu bulunmakta veya sahte bir IATA web sitesine bağlantılar yer almaktadır.

- IATA ürün ve hizmetlerinin kullanıcıları, banka hesabı bilgilerini güncelleme taleplerine karşı her zaman dikkatli olmalı ve değişiklikleri alınan e-postaya yanıt vererek **değil**, güvenilir bir kaynak ile doğrulamaya çalışmalıdır.

- IATA’dan gelmiş görünen iletişimlerin gerçek olup olmadığı konusunda şüpheniz varsa, bu iletişimlerde ödeme talep edilsin ya da edilmesin, lütfen bu iletişimlere yanıt vermeyin. Derhal şu adresten IATA’ya bilgi verin: information.security@iata.org.

- Dolandırıcılık amaçlı en güncel e-posta hesapları hakkında bilgi almak için, lütfen web sayfamızı ziyaret edin.

- Şirketinizi istenmeyen posta, kimlik sahtekarlığı ve kimlik avı gibi risklerden korumak için “DMARC” (Alan Adına Dayalı Mesaj Doğrulama, Raporlama ve Uygunluk) adlı kimlik doğrulama protokolünü kullanmanızı tavsiye ederiz. DMARC, içerdiği iki kimlik doğrulama mekanizması olan Alan Anahtarı Doğrulamalı Posta (DKIM) ve Gönderen Politika Çerçevesi (SPF) sayesinde, e-posta kullanıcılarının İnternet alan adlarının yasal olup olmadığının incelenmesini sağlar.
- DMARC hakkında daha fazla bilgi için lütfen şu adresi ziyaret edin: https://dmarc.org/.

Dolandırıcılık amaçlı internet kullanımı bir suçtur. IATA, kimliğinin kötüye kullanılmasını ciddiye alır.

Lütfen bu bilgileri dikkatli bir biçimde inceleyin. Bunları başta tedarikçi faturalarını ödemekten sorumlu çalışanlar olmak üzere tüm meslektaşlarınızla paylaşmanızı şiddetle öneririz.

Lütfen bu mesaja yanıt vermeyin. Herhangi bir sorunuz varsa, lütfen aşağıdaki iletişim bilgilerini kullanın:

Sorgu Türü	İletişim bilgileri

E-posta Dolandırıcılığı, Kimlik Avı ve Logonun Kötüye Kullanılması	www.iata.org/fraud-prevention **E-posta:** information.security@iata.org
Kart ve Sadakat Dolandırıcılığı	www.iata.org/industryfraudprevention **E-posta:** IFP@iata.org
Müşteri Hizmetleri ve Dolandırıcılıkla İlgili Olmayan Tüm Sorgular	IATA web sitesi: http://www.iata.org. **Müşteri Portalı**: www.iata.org/cs

Dolandırıcılıkla mücadelede yardımınız için teşekkür ederiz.