Phishing Farkındalık Sunumu

Kişisel Bilgileri Korumak İçin Siber Tehditleri Anlamak

Gürsoy Grup Bilgi Teknolojileri

GÜRSOYGRUP

Phishing Nedir?

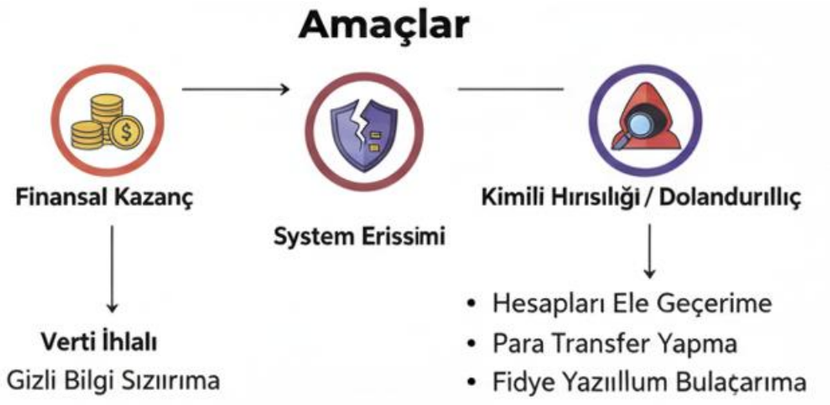
Dijital çağda en yaygın ve tehlikeli siber saldırı yöntemlerinden biri olan phishing, günlük hayatımızda karşılaşabileceğimiz ciddi bir tehdittir. Bu sunum, phishing saldırılarını tanımanızı, kendinizi korumanızı ve şirket verilerinizi güvende tutmanızı sağlayacak temel bilgileri içermektedir.

Her gün milyonlarca phishing e-postası gönderiliyor ve bu saldırılar giderek daha sofistike hale geliyor. Kurumsal çalışanlar ve bireyler olarak, bu tehditleri anlamak ve önlem almak, dijital güvenliğimiz için hayati önem taşımaktadır.

Bu sunumda öğreneceksiniz:

- *Phishing'in tanımı ve nasıl çalıştığı*
- *Sahte e-postaları tanıma yöntemleri*
- *Gerçek hayattan phishing örnekleri*
- *Kendinizi koruma stratejileri*

Phishing'in Tanımı ve Amaçları



GÜRSOY GRUP

Phishing Tanımı

Phishing (oltalama), sahte e-postalar, web siteleri ve mesajlar kullanılarak kişisel bilgilerin (kullanıcı adları, şifreler, kredi kartı numaraları, banka bilgileri) çalınmasını amaçlayan bir siber dolandırıcılık yöntemidir. Adı, balık tutmak için kullanılan "fishing" (balık avlama) kelimesinden gelir.

Kimlik Taklit Taktikleri

Saldırganlar, bankalar, e-ticaret siteleri, devlet kurumları veya tanınmış şirketler gibi güvenilir kurumların isimlerini, logolarını ve iletişim tarzlarını titizlikle taklit ederek kullanıcıları kandırmaya çalışır. Bu taklit o kadar gerçekçi olabilir ki deneyimli kullanıcılar bile bazen aldanabilir.

Etkileri ve Sonuçları

Phishing saldırıları başarılı olduğunda hem bireyler hem de kurumlar için ciddi veri kayıplarına, finansal zararlara, kimlik hırsızlığına ve itibar kaybına yol açabilir. Kurumsal düzeyde, tek bir çalışanın hatası tüm şirket verilerini tehlikeye atabilir.

Farkındalığın Önemi

Phishing'i anlamak, tehdit göstergelerini tanımak ve dikkatli olmak, bilgi güvenliğini korumak ve saldırılardan kaçınmak için hayati öneme sahiptir. Bilinçli bir kullanıcı, en güçlü güvenlik duvarıdır.

GÜRSOY GRUP

Bir Kimlik Avı (Phishing) E-postası Nasıl Tanınır?

Phishing e-postalarını tanımak, dijital güvenliğinizin ilk savunma hattıdır. Saldırganlar sürekli olarak yeni taktikler geliştirse de, dikkat edilmesi gereken bazı ortak özellikler vardır. Bu özellikleri bilmek, şüpheli bir e-posta aldığınızda alarm zillerinin çalmasını sağlar.

E-postanızı açtığınızda, göndericiye, içeriğe ve istenen eyleme dikkat edin. Eğer bir şeyler "doğru gelmiyor" gibi hissediyorsanız, muhtemelen haklısınızdır. ***Güvenlik şüphe gerektirir*** *- acele etmek yerine, bir adım geri çekilip e-postayı dikkatlice analiz edin.*

> ***Altın Kural:*** *Hiçbir meşru kurum size e-posta yoluyla şifre, kredi kartı bilgisi veya kimlik numarası sormaz. Böyle bir talep aldığınızda, derhal şüphelenmelisiniz.*

Phishing E-postalarının Belirtileri

Şüpheli Gönderen Adresi

Phishing e-postaları genellikle resmi kurumları taklit eden şüpheli veya bilinmeyen adreslerden gelir. E-posta adresi dikkatle incelendiğinde genellikle yazım hataları, fazladan karakterler veya garip alan adları içerir. Örneğin, "destek@bankkka.com" yerine "destek@bankka-guvenlik.xyz" gibi.

Acil Eylem Çağrısı

Mesajlar genellikle hesapların askıya alınması, güvenlik ihlalleri veya şifrelerin acilen güncellenmesi gibi senaryolar kullanarak hemen harekete geçmenizi ister. Bu aciliyet hissi, mantıklı düşünmenizi engelleyerek aceleci kararlar almanıza neden olmayı amaçlar. "24 saat içinde işlem yapmazsanız hesabınız kapatılacak" gibi tehditler tipik örneklerdir.

Yazım ve Dilbilgisi Hataları

Phishing e-postalarında sıkça yazım hataları, bozuk cümle yapıları ve tutarsız dil kullanımı görülür. Profesyonel kurumlar her zaman düzgün Türkçe kullanır ve mesajlarını editörden geçirir. Garip ifadeler, yanlış kullanılan kelimeler veya otomatik çeviri belirtileri alarm vermelidir.

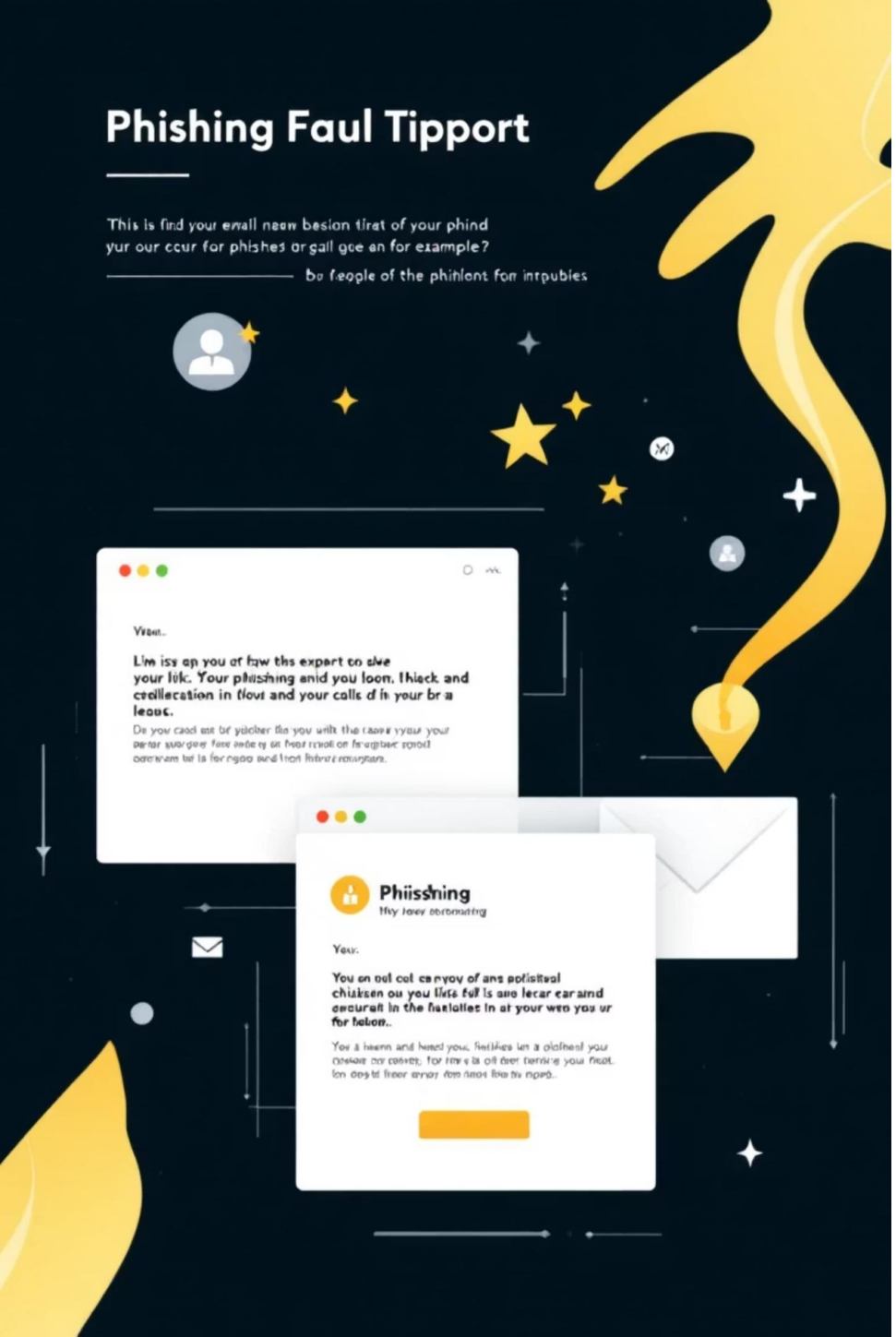
Sahte Bağlantılar ve Ekler

Bu e-postalar, sahte giriş sayfalarına yönlendiren aldatıcı bağlantılar ve zararlı yazılım içeren ekler barındırır. Bağlantının üzerine fare ile geldiğinizde (tıklamadan), gerçek URL'yi görebilirsiniz. Meşru görünen "www.bankaniz.com" yerine "www.bankaniz-guvenlik.malicious-site.com" gibi adreslere dikkat edin.

Ek Uyarı İşaretleri:

- *Genel hitaplar kullanılması ("Sayın Müşteri" yerine isminizin olmaması)*
- *İstenmeyen ekler veya şüpheli dosya formatları (.exe, .zip)*
- *Kişisel bilgi veya şifre talebi*
- *Anormal gönderim saatleri (örneğin gece yarısı)*
- *Tanımadığınız bir hizmetten gelen "hesap doğrulama" talepleri*

GÜRSOY GRUP



Örnek Phishing E-postaları

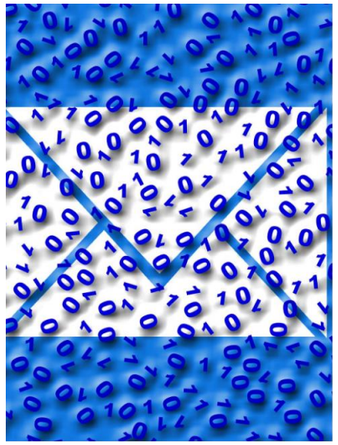
Gerçek dünyadan alınan örnekler, phishing saldırılarının ne kadar çeşitli ve sofistike olabileceğini göstermektedir. Bu bölümde, Türkiye'de sıkça karşılaşılan gerçek phishing vakalarını inceleyeceğiz. Her örnek, farklı taktikler ve kandırma yöntemleri kullanmaktadır.

Neden Gerçek Örnekler Önemlidir?

Teorik bilgi önemlidir, ancak gerçek phishing e-postalarını görmek ve analiz etmek, bu tehditleri tanıma yeteneğinizi önemli ölçüde geliştirir. Takip eden sayfalarda, bankacılık, kargo şirketleri ve kurumsal sistemlerle ilgili gerçek phishing vakalarını detaylı olarak inceleyeceğiz.

Her Örnekte Dikkat Edin:

- *Gönderen e-posta adresindeki anormallikler*
- *URL yapısındaki şüpheli detaylar*
- *Görsel taklit teknikleri*
- *Psikolojik manipülasyon yöntemleri*



Gerçekçi Kimlik Avı Senaryoları

1

Sahte Banka Hesabı Askıya Alma E-postası

Phishing e-postası, tanınmış bir bankadan geliyormuş gibi görünerek "güvenlik nedeniyle hesabınız geçici olarak askıya alındı" mesajı verir. Sahte bir giriş sayfasına yönlendiren bağlantı içerir ve kullanıcı bilgilerini, şifrelerini ve hatta SMS doğrulama kodlarını çalmayı amaçlar. Gerçekçi görünüm için banka logosu, resmi renkler ve jargon kullanılır.

2

Teslimat Başarısızlığı Dolandırıcılığı

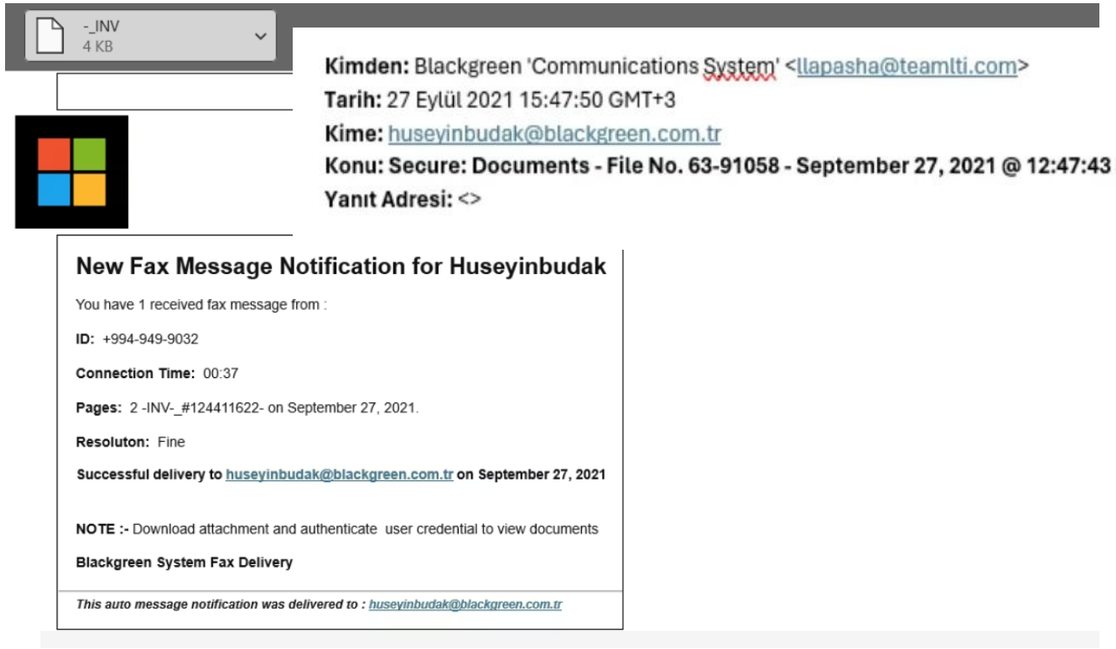
E-posta, Aras Kargo, MNG veya Yurtiçi Kargo gibi popüler kargo şirketlerini taklit eder. "Paketiniz teslim edilemedi, ek bilgi için eki açınız" benzeri mesajlar içerir. Ek dosyalar (.zip, .exe) cihazları zararlı yazılımlarla (ransomware, keylogger) enfekte ederek tüm sistem kontrolünü ele geçirmeyi hedefler.

3

Kurumsal Şifre Sıfırlama Talebi

Phishing e-postası, şirketinizin BT departmanı veya insan kaynakları birimi gibi davranarak "zorunlu güvenlik güncellemesi için şifrenizi sıfırlamanız gerekiyor" mesajı gönderir. Sahte bir şirket içi portala yönlendirir ve kurumsal kimlik bilgilerinizi ele geçirmeyi amaçlar. Bu tür saldırılar, şirket içi verilere erişim sağlayarak büyük kurumsal güvenlik ihlallerine yol açabilir.

Kurumsal Phishing Örneği: Gursoygrup Vakası



Sahte Microsoft Fax Bildirimi

Microsoft e-posta imzası ile gelen bu fax bildirimi e-postası klasik bir phishing örneğidir. Saldırgan, güvenilir bir platform olan Microsoft'u kullanarak kurbanları kandırmaya çalışmaktadır.

01

Gönderen İsmi Aldatmacası

*Gönderen kişi adı **<Blackgreen 'Communications System'>** görünüyor*

02

Gerçek E-posta Adresi

*E-posta üzerine tıklamadan fare ile geldiğimizde **<llapasha@teamlti>** sahte adresini görüyoruz*

03

İlişkisiz Alan Adı

Bu adres ne Blackgreen firması ile ne de Microsoft ile alakalı değildir

04

Sahte Alıcı ve Ek

*Aktif olmayan **huseyinbudak@blackgreen.com.tr** adresine fax gelmiş gibi gösteriliyor ve bilinmeyen bir ek dosyası var*

4

Kritik Uyarı İşareti

Bu örnekte dört farklı phishing göstergesi bir arada bulunmaktadır

100%

Şüphe Oranı

Bu tür çok katmanlı aldatmacalar %100 phishing girişimidir

0

Tıklama Sayısı

Şüpheli eklere ve bağlantılara asla tıklamamalısınız

***Kurumsal Güvenlik Protokolü:** Beklenmedik fax bildirimleri, özellikle ek dosya içeriyorsa, derhal BT departmanınıza bildirilmelidir.*

Hiçbir eki açmadan önce gönderenin kimliğini alternatif bir iletişim kanalı üzerinden doğrulayın (telefon, resmi web sitesi vb.).

Ne Yapmalısınız?

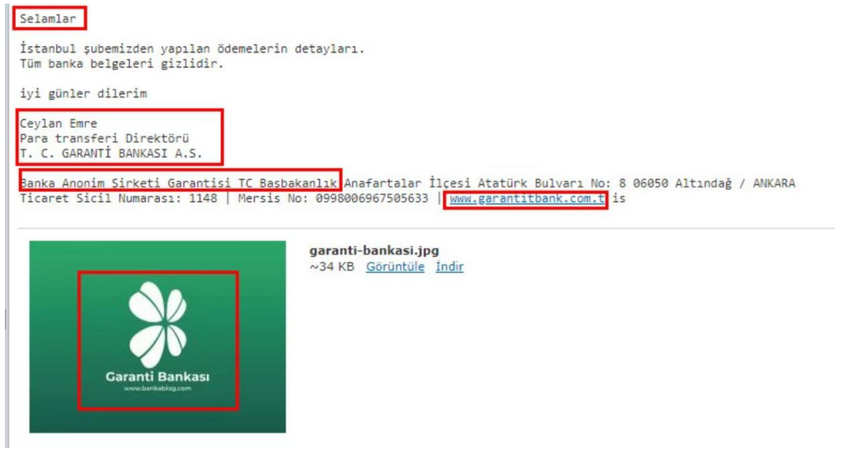
- *E-postayı hemen spam olarak işaretleyin*
- *Eki kesinlikle açmayın*
- *BT güvenlik ekibinize bildirin*
- *E-postayı silmeden önce kayıt altına alın*
- *Meslektaşlarınızı uyarın*

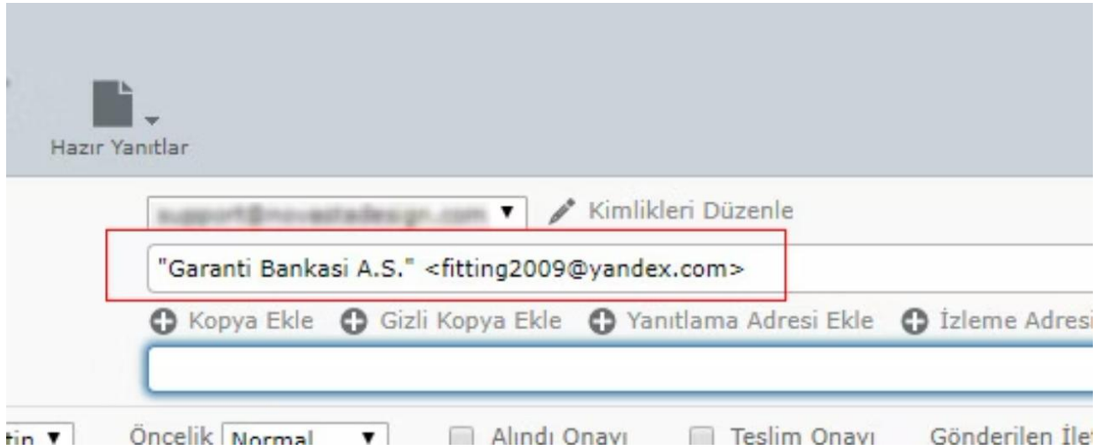
Korunma Stratejileri

- *E-posta güvenlik filtrelerini güncel tutun*
- *Çalışanlara düzenli phishing eğitimleri verin*
- *Çok faktörlü kimlik doğrulama kullanın*
- *Şüpheli durumları raporlama sistemi oluşturun*
- *Güvenlik protokollerini düzenli gözden geçirin*

GÜRSOYGRUP

Garanti Bankası Phishing Örneği: İki Kritik Hata





1 Sahte İletişim Bilgileri

*E-posta imzasının altında bulunan adres ve web sitesi bilgileri uydurma olduğu gibi yanlış da yazılmıştır. Ancak **algı probleminden dolayı beynimiz** bu bilgileri hızlı bir şekilde tarayarak "doğru" gibi yorumlayıp sizi kandırabilir.*

Dikkatli bakmadığınızda, görsel düzen ve logo kullanımı sayesinde gerçek gibi görünen bu detaylar aslında tamamen sahte olabilir. Her zaman yavaşlayın ve detayları kontrol edin.

2 Gizlenmiş Gönderici Adresi

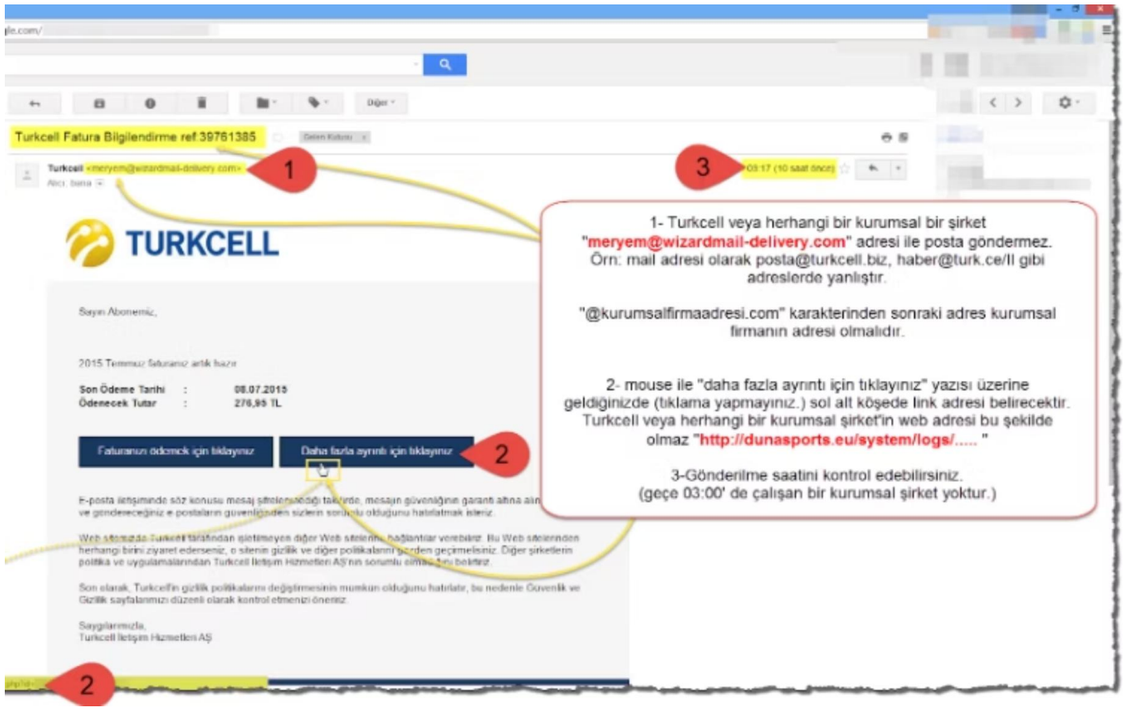
Deneyimli bir kullanıcı iseniz, e-postanın gerçekten Garanti Bankası tarafından mı gönderildiğini öğrenmek için gönderen adının üstüne basmanız yeterlidir.

*Bu örnekte, spam üreticisi e-posta başlığındaki "title" öğesini **"Garanti Bankasi A.S."** olarak girip gerçek gönderen e-posta adresini **"fitting2009@yandex.com"** olarak gizlemeye çalışıyor.*

E-posta başlıklarındaki "title" öğesi, Outlook ve benzeri uygulamalarda e-posta sahibinin ismini kolay tanınması için gösterir, ancak gerçek adresi değiştirmez.

***Öğrenilen Ders:** Görünüş aldatıcı olabilir. Bir e-postanın profesyonel görünmesi, onun meşru olduğu anlamına gelmez. Her zaman teknik detayları kontrol edin - gönderen adresi, bağlantı URL'leri ve e-posta başlıkları sizin en iyi doğrulama araçlarınızdır.*

Turkcell Phishing Örneği: Detaylı Analiz



1

Sahte E-posta Adresi Analizi

*Turkcell veya herhangi bir kurumsal şirket, **"meryem@wizardmail-delivery.com"** gibi adreslerden e-posta göndermez. Aynı şekilde **posta@turkcell.biz, haber@turk.ce/ll** gibi adresler de yanlıştır ve phishing girişimidir.*

*Doğru bir kurumsal e-posta adresi mutlaka **@kurumsalfirmaadresi.com** şeklinde olmalıdır. Örneğin, Turkcell'den gelen meşru e-postalar **@turkcell.com.tr** uzantısına sahip olacaktır.*

2

Bağlantı URL'si Kontrolü

***"Daha fazla ayrıntı için tıklayınız"** gibi bağlantı metinlerinin üzerine **fare (mouse) ile geldiğinizde** (kesinlikle tıklamayın!), tarayıcınızın sol alt köşesinde gerçek bağlantı adresi görünür.*

*Örneğin: **http://dunasports.eu/system/logs/...** gibi bir adres, Turkcell veya başka bir Türk kurumsal firmasının adresi kesinlikle olamaz. Meşru bir Turkcell bağlantısı **https://www.turkcell.com.tr/...** şeklinde başlamalıdır.*

***Önemli Güvenlik İpucu:** Şüpheli bir bağlantıyı asla tıklamayın. Eğer bir kurumun size gerçekten ulaşıp ulaşmadığından emin değilseniz, o kurumun resmi web sitesine tarayıcınızdan doğrudan gidin veya müşteri hizmetlerini arayın.*

GÜRSOY GRUP