



# olta.la

## AĞUSTOS AYI GÜNCEL OLTALAMA RAPORLARI



OLTALAMA  
SİMÜLASYONU



EĞİTİM



OLAY  
MÜDAHALE

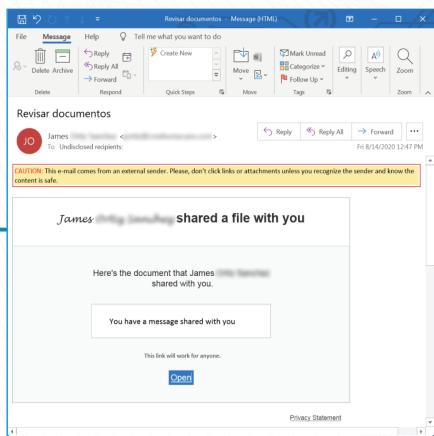


GÜVENLİ ELEKTRONİK  
HABERLEŞME SİMÜLASYONU

## Zafiyet 1: Canva Platformu Üzerinden Yapılan Saldırı

Canva Platformu, grafik tasarım tasarımları yapmak için kullanılan görsel ve kullanışlı bir platformdur. Saldırganlar dosya paylaşım ya da içerik paylaşım platformları üzerinden zararlı bağlantı adresi ya da zararlı dosyaları gizleyerek saldıruları gerçekleştirmektedir. Bu e-postada, Canva platformu içerisinde tasarlanan ve yine bu uygulama üzerinden servis edilen kötü amaçlı içerik ile saldırı düzenlenmiştir.

### Adım 1:



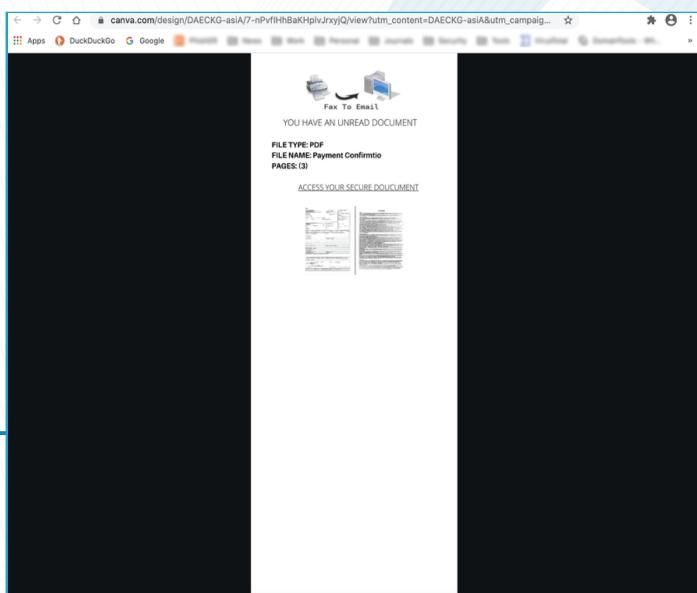
Microsoft Sharepoint'ten bir dosya paylaşım bildirimini taklit ederek gönderilen e-posta ile kimlik avı saldırısının ilk adımı gerçekleştirilmiş.

Gönderen adı **“James”**, gönderen konusu **“Revisar Documentos”** olarak İspanyolca yazılmış **“Belgeleri Gözden Geçir”** anlamında olan bir ifade kullanılmış. E-posta içerisinde ise, James tarafından bir dosya paylaşımı yapıldığı bilgisi verilmiştir.

### Dikkat edilmesi gerekenler:

E-posta içerisinde bulunan **“OPEN”** butonu gerçek bir bağlantı adresi gibi görünse de bağlantı adresinin üzerine gelerek yönlendirilen sayfa kontrol edilmelidir.

### Adım 2:



“OPEN” linkine tıkladıktan sonra açılan sayfada, paylaşılan dosyanın genel bilgileri ve dosyaya erişebilmek için bir bağlantı adresi kullanılmıştır. Yönlendirilen sayfanın adresi **“canva.com/design/DAECKG-asiA/7-nPVFH...”** olarak Canva.com platformunda tasarlanmış bir içeriğin adresidir. Eğer Canva platformunu kullanmadıysanız, platformda herhangi bir içerik oluşturduğunuzda bu içeriğin paylaşımının yapılması için bir bağlantı adresi oluşturulur. Siber saldırganlar da, bu bağlantı adresini kullanarak tasarladıkları içeriği bu adres üzerinden servis etmektedir.

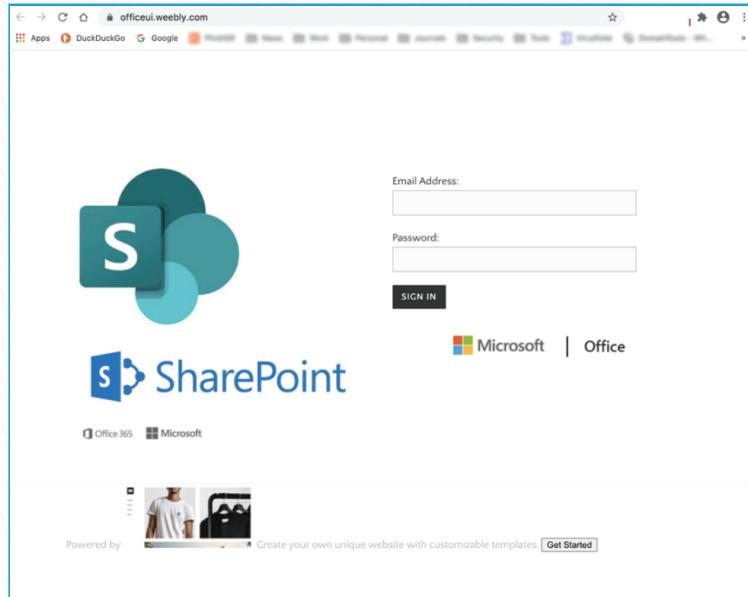
### Dikkat edilmesi gerekenler:

E-posta içerisinde dosya paylaşımı ile ilgili bir içerik varsa e-posta içerisindeki link ile yönlendirilen sayfanın gittiği adres kontrol edilmelidir. **Yönlendirilen sayfadaki adresi incelediğinizde “https” alan adını görmeniz güvenli olduğu anlamına gelmemektedir. Uygulamanın ne uygulaması olduğu ve ne amaç ile kullanıldığı mutlaka araştırılmalıdır. Canva görsel içeriklerin oluşturulmasına olanak tanıyan bir grafik tasarım platformudur. Dosya paylaşımı için kullanılamaz.**

Dikkat edilmesi gereken bir diğer önemli nokta ise açılan sayfadaki dosya indirme ekranıdır. Saldırıda kullanılan ekran hiç alışık olmadığımız sıradışı bir içerik ve görselle sahiptir.

Yazım kurallarına dikkat edilmelidir. Dosyaya erişebilmek için kullanılan “Access Your Secure Document” ifadesinde “Document” olarak yazılması gereken kelime “Document” şeklinde yazılarak yazım hatası bulunmaktadır.

### Adım 3:



“Access Your Secure Document ” linkine tıklama aksiyonu sonucunda, web sitesi oluşturma uygulaması olan Weebly üzerinden officeui.weebly.com alan adı ile bir internet sitesi tasarlanmıştır. Bu site üzerinden de, kullanıcıların bilgilerini ele geçirmek hedeflenmiştir.

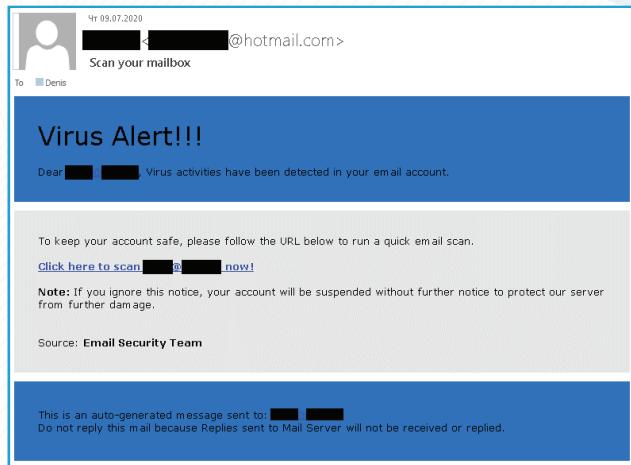
Yönlendirilen sayfada **adres çubuğundan** bağlantı adresi kontrol edilmelidir. “Weebly” alan adına sahip bir sayfa güvenilir gözükse de sayfa içerisinde kullanılan **Microsoft Share Point** ürününün giriş sayfasının imajının verilmesi saldırı amaçlı bir sayfa olarak oluşturulduğunu göstermektedir.

Web sayfasının alt kısmında verilen reklam görseli ve “Create your own unique website” ifadesi sayfanın kurumsal bir platforma ait olmadığını göstermektedir.

### Zafiyet 2: Zafiyet 2: E-posta Tarayıcısı Kimliğinde Tasarlanan Sitelere Yönlendirilme

Siber saldırganlar tarafından e-posta içeriğinde virüs tespit edildiğine dair kullanıcıları panik ve korkuya kapılmasına neden olan saldırı düzenlemiştir. Bir kuruluş tarafından gönderildiği izlenimi veren bu e-postanın içerisinde, e-postaların güvenlik taramasının yapılabileceğini gösteren bir bağlantı adresi ile saldırıyı gerçekleştirmiştir.

### Adım 1:



E-posta konusu olarak “Scan your mailbox” kullanılmış; e-posta içerisinde, virüs alarmı “Virus Alert!!!” ifadesi kullanılarak belirtilmiş. E-posta içerisinde yer alan “Email Security Team” ifadesi bir kurumdan gelmiş mesajı verse de gönderenin alan adı incelendiğinde “Hotmail.com” hesabından gönderilmiştir. E-posta içerisinde, e-posta güvenlik taramasının gerçekleştirilmemesi halinde hesaplarına erişim olmayacağı belirten bir ifade kullanılmıştır. **Acılıyet duygusu** ile içerikte verilen bağlantı adresine tıklanması amaçlanmıştır.

## Dikkat edilmesi gerekenler:

Gönderenin alan adı “**@hotmail.com**” hesabından gönderilmesi kişisel bir hesaptan gönderildiğini belirtmektedir. **“Email Security Team”** ifadesi ile bir kurumdan gönderildiği mesajı verilse de kuruma dair hiçbir bilgi yoktur. Kurum adı olsa da Gönderen alan adı mutlaka kontrol edilmelidir. **Hiçbir kurum kendi alan adını barındırmayan bir adresten e-posta göndermez.**

### Adım 2:



E-posta içerisinde bulunan linke tıklandığında e-posta tarayıcısı gibi görünen bir web sitesine yönlendirme yapılmıştır. Web sitesinin gerçek ve yasal olduğuna kullanıcıyı ikna etmek için **birçok antivirus sağlayıcısının logosu** kullanılmıştır.

Ayrıca siteyi kişiselleştirmek için **alicinin e-posta adresi** kullanılmıştır. **“Complete Scan”** butonuna tıkladıktan sonra **“Confirm your account below to complete Email scan & delete infected all files”** uyarısı ile tarama işlemi durdurularak kullanıcıdan e-posta hesabını ve şifresini iletmesi istenmektedir.

## Dikkat edilmesi gerekenler:

- E-posta şifreniz kişiseldir. Kesinlikle ikinci bir tarafla paylaşılmamalıdır.
- Yönlendirilen sayfanın adresi kontrol edilmelidir. Https kullanıldıysa bile adreste bulunan alan adı ile sayfa içeriği incelenmelidir.
- Sayfa içerisinde yazım yanlışı olmamasına dikkat edilmelidir.
- Sayfa içerisinde başka bir bağlantı adresi varsa mutlaka bağlantı adresinin üzerine gelerek yönlendirilecek olan adres kontrol edilmelidir.

## Zafiyet 3: Outlook Güncellemeye Kimlik Bilgileri Saldırıları

Siber saldırganlar, kurum çalışanlarının Microsoft hesaplarını sürekli hedef almaktadır. Saldırganlar için bu hesaplar hassas iş bilgilerini barındıran önemli bir hazinedir.

## Adım 1:

From: [REDACTED]  
Sent: Tuesday, July 07, 2020 4:16 AM  
To: [REDACTED]  
Subject: New Microsoft Outlook for Staff/Employee

Welcome to the New Microsoft Outlook for Staff/Employee.

All Staff/Employee are expected to migrate to the New 2020 Microsoft Outlook Web Portal to enable access Click on [Login here](#) and login to migrate immediately and Complete the upgrade:

- Access the new staff directory
- Access your pay slips and P60s
- Update your ID photo
- E-mail and Calendar Flexibility
- Connect mobile number to e-mail for voice mail

Important notice: All staffs/Employee are expected to migrate within 24 hours to avoid delay on mail delivery.

On behalf of IT Support. This is a group email account and it's been monitored 24/7, therefore, please do not ignore this notification, because it's very compulsory.

Sincerely,  
Administrator Service System.  
Microsoft Outlook Team

Saldırı Microsoft Outlook tarafından gönderilmiş, resmi bir e-posta gibi gösterilmektedir. Outlook hizmetlerini **24 saat içinde “yükseleme”** istenir. İstenilen aksiyon yapılmadığı takdirde hesaplarından e-posta gönderim işlemlerinin erteleneceği belirtilir.

## Dikkat edilmesi gerekenler:

E-posta içerisinde; panik ve aciliyet anlamına gelen **“24 saat içinde yükseltme”** ya da **“E-posta gönderiminiz gecikebilir”** gibi ifadeleri görüyorsanız **dikkatli olmalısınız**. E-posta ne kadar Microsoft Outlook ekibinden gelmiş gibi gözüksede aciliyet duygusu ile düşünmeden istenilen aksiyonun gerçekleştirilemesine teşvik etmektedir.

## Adım 2:



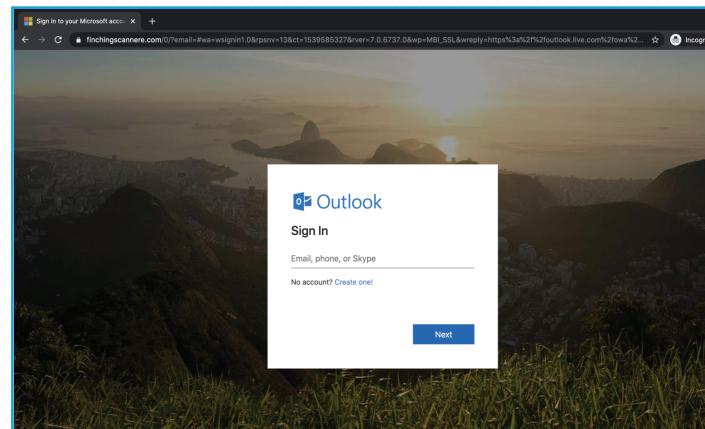
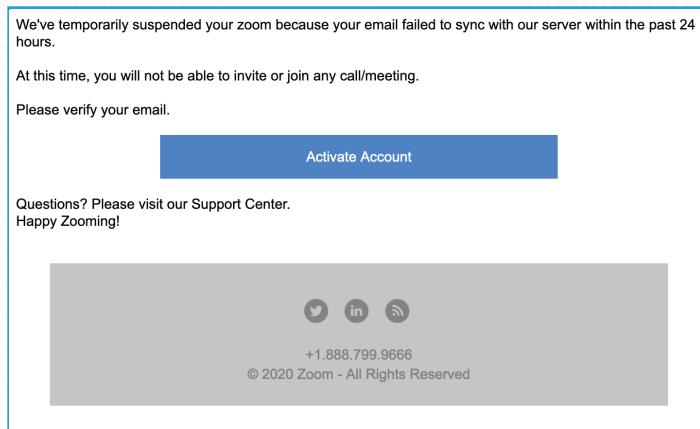
E-posta içerisinde bulunan bağlantıya tıklandığında bir web sitesinde barındırılan sahte bir Outlook oturum açma sayfasına yönlendirilir. Web sitesinin adresi, **“http://owasharepoint.godaddysites.com/”** olarak kullanılmıştır. Kullanıcı bilgi girişi yaptıktan sonra **“Next”** butonuna tıklandığında **“Yükseltme önumüzdeki 48 saat içinde tamamlanacaktır”** şeklinde bir uyarı vermektedir.

## Dikkat edilmesi gerekenler:

Yönlendirilen web adresinin **“https”** ile başlamasına dikkat edilmelidir. Yönlendirilen sayfanın içeriği Microsoft Outlook giriş sayfası gibi gözüksede adres çubuğundan sayfanın adresi incelendiğinde **“http://owasharepoint.godaddysites.com/”** ‘dur. Gerçek bir Microsoft Outlook giriş sayfası **“godaddysites.com”** alan adını kullanmamaktadır. Sayfa içerisinde yeni bir portaldan bahsedilse bile alan adının Outlook etki alanında olması gerekmektedir. **Yönlendirilen sayfa içeriği ile adres çubuğundaki alan adının aynı etki alanında olduğundan emin olunmalıdır.**

Unutmayın ki hiçbir kurum ya da kuruluş sizden **şifrenizi istemez!**

## Zafiyet 4: Sahte Zoom Saldırısı 1



**Adım 1:** Gönderilen e-postada Zoom alan adını taklit eden bir e-posta adresinden gönderilmiştir. Zoom'dan gelen otomatik bildirimini kullanarak kullanıcının hesabını aktif etmesini istemektedir. E-posta içerisinde yer alan bağlantı adresine tıklayarak aktivasyon işlemi yapılmazsa Zoom hizmetlerini kullanamayacağı belirtilmektedir.

**Adım 2:** E-posta içerisindeki bağlantıya tıklandığında sahte olarak tasarlanmış başka bir etki alanında bulunan sayfaya yönlendirilmektedir. Sayfa içeriği incelendiğinde, **Microsoft Giriş sayfası** gibi gözüke de adres incelendiğinde **“finchingscannere.com”** şeklinde **farklı bir alan adında** olduğu görülmektedir.

### Dikkat edilmesi gerekenler:

Yönlendirilen sayfanın içeriği Microsoft Outlook giriş sayfası gibi gözüksede adres çubuğundan sayfanın adresi incelendiğinde **“finchingscannere.com”** ‘dur. Gerçek bir Microsoft Outlook giriş sayfası **“https://login.live.com/”** şeklinde bir alan adına sahiptir. **Yönlendirilen sayfa içeriği ile adres çubuğundaki alan adının aynı etki alanında olduğundan emin olunmalıdır.**

**Unutmayınız, e-posta hesabınız ve şifreniz ile başka bir uygulama üzerinden giriş yapmak bilgilerinizi tehlikeye sokmaktadır.**

## Zafiyet 5: Sahte Zoom Saldırısı 2

Zoom uygulamasının kullanımının artmasıyla birlikte Zoom üzerinden yapılan saldırılarda artmaktadır. Siber saldırganlar, Zoom uygulamasından gönderilen resmi içerikleri kullanarak saldırı gerçekleştirmektedir. Bu kapsamında, bir toplantı davetinin ayrıntılarına ulaşmak için paylaşılan bir bağlantı adresi ya da bir toplantı başlatmak için indirilmesi gereken ek bir dosya olduğunu belirten içerikler kullanılmaktadır.

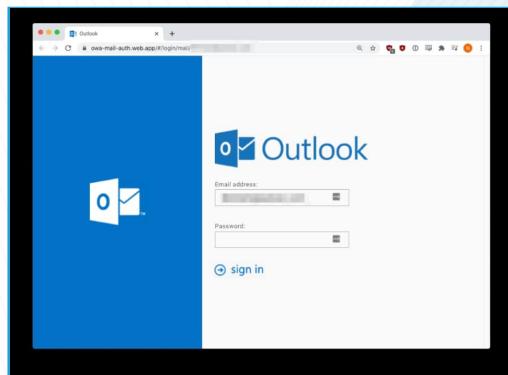
## Adım 1:

The screenshot shows an email from Zoom titled "Zoom Video Conference For [REDACTED]". The body of the email reads: "Hi [REDACTED], You have received a Zoom video conferencing invitation. Zoom Meeting ID: 367193657". Below the email is a block of WHOIS data for the domain ZOOMCOMMUNICATIONS.COM.

```
Domain Name: ZOOMCOMMUNICATIONS.COM
Registry Domain ID: 2522706729_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.meshdigital.com
Registrar URL: http://www.meshdigital.com
Updated Date: 2020-05-21T00:04:58Z
Creation Date: 2020-05-06T12:05:20Z
Registry Expiry Date: 2021-05-06T12:05:20Z
Registrar: Mesh Digital Limited
Registrar IANA ID: 1398
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.DOMAINHASEXPIRED.COM
Name Server: NS2.DOMAINHASEXPIRED.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-07-28T13:55:48Z <<<
```

E-posta içeriği, Zoom kurumundan gelen ve toplantıya davet etmek amacındadır. Resmi olarak Zoom tarafından gönderilen içeriğin birebir aynısı taklit edilmiştir. E-postanın başlık bilgilerinde görüldüğü gibi gerçek imajı vermek için kullanılan alan adı zoomcommunications.com'dur.

## Adım 2:



E-posta içerisinde bulunan bağlantı adresine tıklandığında, kullanıcıların Zoom bilgileri sorulması gerekikten gerçek görünümü Outlook Web App oturum açma sayfasına yönlendirilmiştir. Açılan sayfanın adresi incelendiğinde "**"owa-mail-auth.web.app"**" şeklinde hazırlanmıştır.

Sayfa içeriği ne kadar Outlook giriş sayfası gibi gözükse de web adresi incelendiğinde kullanıcıya güven kazandırmak için "**"web.app"**" alan adı üzerinden oluşturulmuş "**"owa-mail-auth"**" alt alan adı ile Firebase içerisine entegre edilerek servis edilen saldırı amaçlı oluşturulmuş bir internet sayfasıdır.

**Dikkat edilmesi gerekenler:**

Yönlendirilen sayfanın içeriği Microsoft Outlook giriş sayfası gibi gözükse de adres çubuğundan sayfanın adresi incelendiğinde "**"owa-mail-auth.web.app"**" adresi görülmektedir. Bir kurum tarafından kullanılan Outlook Web Application da adres "**"owa.kurumadi.com"**" olacak şekilde kendi alan adlarından servis edilmektedir. Bu kapsamda, saldırı örneği için dikkat edilmesi gereken en önemli kriter kurumların kendi alan adını barındıran bir Web Outlook Uygulamasına sahip olmasıdır.