SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

SİBER

SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

KOCAELİ

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

BİRİMLE İLGİLİ GENEL BİLGİLER

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Siber Suçlarla Mücadele Şube Müdürlüğümüz, ilimiz Derince ilçesinde bulunan İl Emniyet Müdürlüğü yerleşkesinde faaliyet göstermektedir.

Telefon & Faks : 0(262) 229 0706
e-posta:kocaeli155@egm.gov.tr
siber.kocaeli@egm.gov.tr

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

KARŞILAŞILAN SUÇ TÜRLERİ

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

- Banka/Kredi Kartı Kopyalama Olayları
- Sahte Siteler ve Formlar Aracılığıyla İnternet Bankacılığı Hesabından Para Aktarımı veya Kredi Kartından Harcama Olayları
- Sunucu/Server Ele Geçirme Olayları
- Sahte E-Posta Aracılığıyla Dolandırıcılık
- Kişisel Verilerin Ele Geçirilmesi

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Banka/Kredi Kartı Kopyalama Olayları

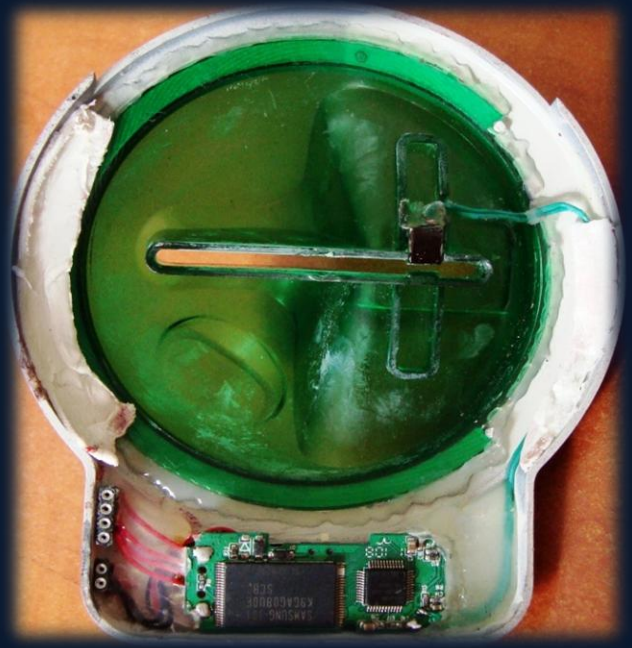
SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Banka/Kredi kartı kopyalama olayları; ATM'ler üzerinde düzenek yerleştirilmesi yöntemiyle, POS cihazı görünümlü sahte cihazlar aracılığıyla gerçekleştirilmektedir.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Banka/Kredi Kartı Kopyalama Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM



Yandaki resimlerde şüpheliler tarafından ATM'lere takılan kart kopyalama aparatları yer almaktadır. ATM'ye dışarıdan bakıldığında anlaşılması zordur.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Banka/Kredi Kartı Kopyalama Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Banka/Kredi Kartı Kopyalama Olaylarına Karşı Alınacak Tedbirler;

- Kapıda ödeme yaparken 2. bir POS cihazı ile işlem yapılmamasına özen gösterilmeli,
- ATM'de işlem yapıldığı esnada kartı ATM'ye takmadan önce kart giriş haznesini elle kontrol edilmeli,
- Restoranlarda yemek yedikten sonra ödemeyi banka/kredi kartı ile yapacaksak POS cihazını masaya isteyelim ya da kart ile bizzat POS cihazından ödeme yapmak üzere biz gidelim. Bazı art niyetli çalışanlar tarafından kart kopyalama olayları gerçekleştirildiği tespit edilmiştir.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sahte Site ve Formlar İle Kimlik Avı Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Bu tarz olaylarda kullanıcının eposta adresine Fatura Ödeme, İnternet Bankacılığı Güncelleme gibi başlıklarla içerisinde sahte siteye yönlendirici linklerin bulunduğu mail gönderilerek bilgiler çalınır.

Bu web siteleri genellikle kredi kartı ile fatura ödeme, internet bankacılığına giriş vb. içeriklidir.

Sahte Site ve Formlar İle Kimlik Avı Olayları

Yukarıda yer alan resim sahte bir fatura bilgilendirme mailinden alıntıdır.

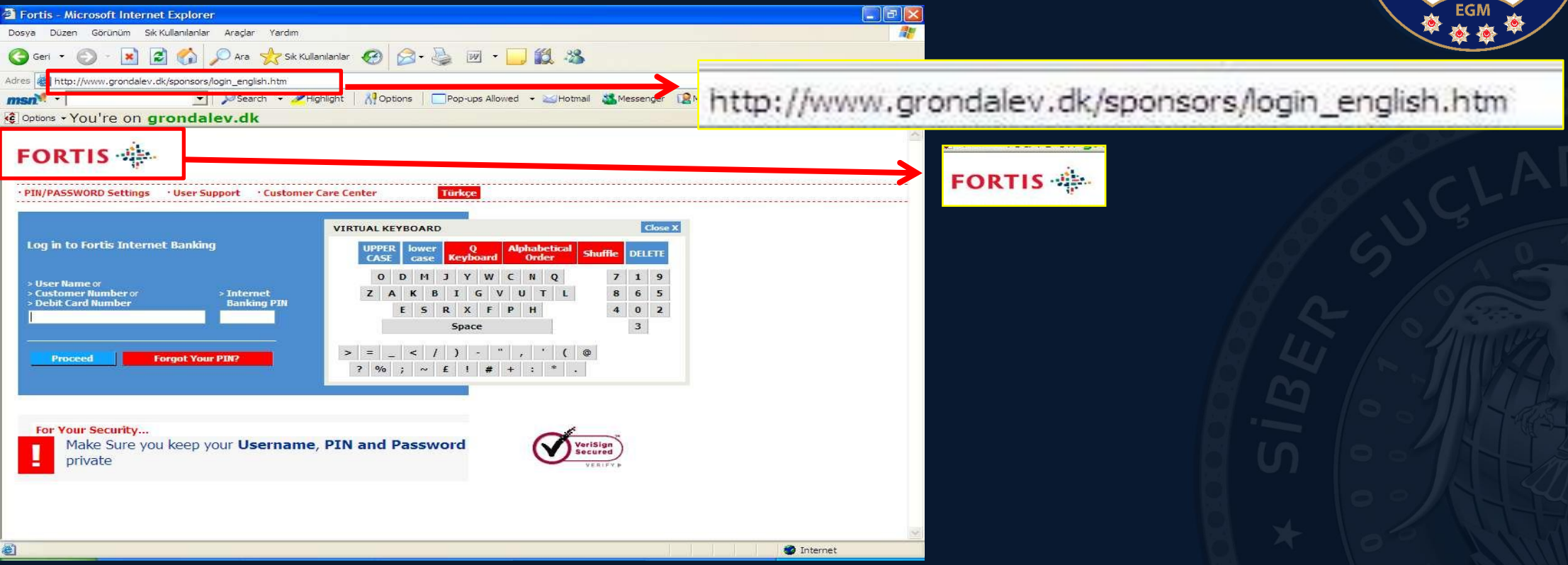
Görüldüğü üzere Müşteri ad-soyadı bilgisi tam değildir.

Fatura tutarı sizi bir anlık telaşlandırmak amacıyla çok yüksek yazılmıştır.

E-Faturanızı görüntülemek için tıklayın ibaresi yer alan link ile sizi başka bir sayfaya yönlendirmek istemektedir.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sahte Site ve Formlar İle Kimlik Avı Olayları



Yukarıda yer alan resim sahte bir internet bankacılığı giriş sayfasından alıntıdır.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sahte Site ve Formlar İle Kimlik Avı Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

GERÇEK

https://acs.bkm.com.tr/mdpayacs/pareq

Verified by VISA

TÜRKİYE İŞ BANKASI

Lütfen şifrenizi giriniz

Üye İşyeri : LIMANGO DIS TICARET
Tutar : TRY 61.98
Tarih : 20130430 12:14:02
Kart Numarası : XXXX XXXX XXXX 0092
Kişisel güvence mesajı (PAM) : 0 *** ***4440

İşlem şifreniz 0 xxx xxx4440 olan cep telefonunuza gönderilecektir.
Lütfen tqhw2845 referans numaralı alışveriş şifrenizi giriniz.

Yardım | Vazgeç | Gönder

Bu bilgiler İşyeri ile kesinlikle paylaşılmamaktadır.

SAHTE

Verified by VISA

Lütfen telefonunuza gönderilen 3D şifrenizi giriniz.

Üye İşyeri : FATURA ÖDEME VE SORGULAMA SERVİSİ
Tarih : 11:35, Salı, Eylül 30, 2014
Kart Numarası : XXXX XXXX XXXX XXXX
Kişisel güvence mesajı (PAM) : 0 5** *** ****

5 dakika içerisinde bankanıza kayıtlı cep telefonunuza
3D secure şifreniz gönderilecektir.
Lütfen telefonunuza gelen şifrenizi giriniz.

Yardım | Vazgeç | Gönder

Lütfen Şifreniz size ulaşana kadar bu sayfayı kapatmayınız.
Şifreniz 5 dakika içerisinde size ulaştırılacaktır.
Şifrenizi büyük küçük harf ayrımına dikkat ederek giriniz.

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Phishing/Pharming Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

SAHTE SİTELERE KARŞI ALINACAK TEDBİRLER

- İşlem yaptığımız site adresi ile işlem gerçekleştirmek istediğimiz site adresinin aynı olmasına dikkat edilmeli,(ÖRNEK: **garantibank.com.tr/ garantibnk.com.tr**)

- Online alışverişler esnasında banka tarafından telefonumuza gönderilen 3D şifresi referans numarası ile ekranda yer alan referans numarasının kontrol edilmeli,

- E-Posta adresinize gelen fatura bilgilendirme, banka iletişim bilgileri güncelleme gibi şüpheli epostaları açmamaya, açtığınız durumlarda eklentileri indirmemeye ve eposta içeriğinde yer alan yönlendirme linklerine tıklamamaya dikkat edilmeli,

- Güncel ve Lisanslı antivirüs programı kullanmaya özen gösterilmeli,

Sunucu/Server Ele Geçirme Olayları

Kötü niyetli bilgisayar kullanıcıları, şirketlerin;

- Personel kayıtları,

-Muhasebe ve müşteri kayıtları,

gibi bilgilerinin bulunduğu sunucu bilgisayarları ele geçirerek dosyaları şifrelemektedirler.

Şifreleme sonrası sunucu ekranına ‘benioku.txt’ isimli bir dosya bırakır.

Dosya içerisinde kendisiyle iletişime geçmeniz için size bir eposta adresi bırakır.

Yapılan görüşmenin ardından para talep eder ve bu parayı çeşitli ödeme yöntemleri ile gönderilmesin isterler,

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sunucu/Server Ele Geçirme Olayları

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Sunucu Ele Geçirme Olaylarına Karşı Alınacak Tedbirler;

- Sunucu bilgisayarın şifresini genel olarak kullanılan **asd12345** gibi basit şifreler yerine **Mk.1874@!/*-+215** gibi karmaşık yapıda ve kullanıcı adlarını Admin, Yönetici gibi isimler yerine size özel isimler kullanılmalı,

- Sunucu bilgisayarın periyodik zamanlarda yedeği alınmalı ve bu yedeğin sunucu ile olan bağlantısı kesilmeli,

- Sunucu bilgisayar sistemine firewall(güvenlik duvarı) kurdurulmalı ve güncellenmeli,

- Uzaktan erişim yapılmasına izin verilen kişilerin IP bilgilerinin sisteme tanımlanmalı,

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sahte E-posta Aracılığıyla Dolandırıcılık

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Art niyetli bilgisayar kullanıcıları bilgisayarlara gönderdikleri zararlı yazılım ile e-posta trafiğinizi kontrol altına alarak firmalar ile yapmış olduğunuz yazışmalara erişebilmektedirler.

Karşı firma ile yapmış olduğunuz anlaşma neticesinde gönderdiğiniz proformayı karşı tarafa ulaşmadan almakta ve sahte bir proforma oluşturarak **banka hesap bilgileri** değiştirmektedir.

Sonrasında ise anlaşmış olduğunuz firma hesap numarasını teyit etmeden para gönderimi yaptığında şüpheli/şüpheliler tarafından para çekilmektedir.

Bu durum bazen sizin eposta sisteminiz üzerinden işlerken bazen de şüpheliler sizin veya müşterinizin eposta adresinize benzer bir hesap açarak işlemlerini yapmaktadır.

Örneğin; **siberkocaeli@egm.gov.tr** yerine
siberkcaeli@egm.gov.tr gibi

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Sahte E-posta Aracılığıyla Dolandırıcılık

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Sahte e-posta Olaylarına Karşı Alınacak Tedbirler;

- Öncelikli olarak karşı firma ile sadece eposta üzerinden değil telefon görüşmesi, skype görüşmesi gibi farklı yollarla görüşerek teyit alınmalı,
- Anlaştığınız firmanın size para göndermeden önce hesap numarasını teyit etmesini isteyiniz,
- Bilgi İşlem Departmanınız varsa zaman zaman sistemlerinize erişim sağlayan IP numaralarını kontrol ettiriniz,

SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

Örnek Olay

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

Müşteki A isimli firma tarafından mal alım satım yaptığı müşterisi ABCDE FİNANCE S.A. isimli şirkete 05/04/2015 tarihinde 800 numaralı fatura kesildiği, bu faturada paranın yatırılacağı hesap olarak AA belirtildiği, bu hesabın müştekiye ait olduğu, müştekinin bilgisi dışında faturanın değiştirildiği ve karşı firmaya sahte fatura gönderildiği, bu faturada müşteki ile ilgisi bulunmayan Kuveyt Türk Katılım Bankası A.Ş. nezdinde bulunan TR36 XXXX XXXX XXXX XXXX XXXX XX IBAN numaralı hesaba paranın gönderilmesinin sağlandığı, bu hususun müşteki firmanın bilgisi dışında olduğu, yine müştekiye gelmesi gereken paranın Türkiye Garanti Bankası A.Ş. nezdinde bulunan AB TURİZM ve XY AJANS isimli hesaba aktarılması sağlanarak firmanın toplamda 750.000,00 TL zarara uğratılmıştır.

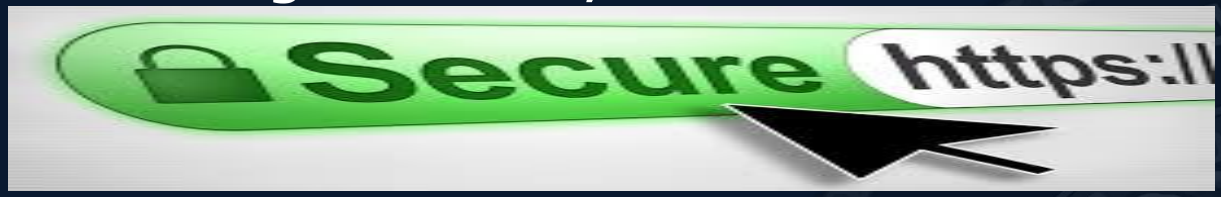
SİBER
SUÇLARLA MÜCADELE ŞUBE MÜDÜRLÜĞÜ

TAVSİYELER

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI
EGM

✓Kişisel bilgilerin paylaşılmamasına özen gösterilmeli,

✓Güvenli internet kullanılmalı,



✓İnternette gezinirken ihtiyaç duyduğunuz yazılım ve uygulamalardan ücretsiz olanlara kullanılmamalı,

✓Tanımadığınız kişilerden gelen veya şüpheli görünen epostaları açmayın, eklerini indirmeyin,

✓Güçlü parolalar, LİSANSLI VE GÜNCEL YAZILIMLAR YAZILIMLAR kullanılmalı,

SUNUM BİTMİŞTİR

TEŞEKKÜR EDERİZ.