Her Yaşta Siber Güvenlik: Dijital Dünyada Güvende Kalmak

Niyazi Doralp, PMP CISA CFE
https://doralp.ca
nick@doralp.ca

GİRİŞ: DİJİTAL DÜNYADA NEDEN GÜVENLİK ÖNEMLİ?

Teknoloji artık hayatımızın vazgeçilmez bir parçası haline geldi. Akıllı telefonlar, bilgisayarlar, tabletler ve internet ile günlük işlerimizi daha kolay halledebiliyoruz. Bankacılık işlemlerimizi evden yapıyor, sevdiklerimizle görüntülü konuşuyor, alışverişimizi internetten halledebiliyoruz. Ancak bu kolaylıklar beraberinde bazı riskleri de getiriyor.

Norbert Wiener'in 1940'larda ortaya attığı "Cybernetics" kavramından türeyen ve William Gibson'ın 1984'te "Neuromancer" romanıyla popüler hale gelen "siber" dünya, bugün hepimizin içinde yaşadığı bir gerçeklik. Bu dijital evrendeki güvenliğimiz, fiziksel dünyada kapımızı kilitlemeye benzer biçimde önem taşıyor.

Son istatistikler, özellikle ileri yaştaki bireylerin siber dolandırıcılık vakalarında daha fazla maddi kayıp yaşadığını gösteriyor. Bu rehber, kendinizi bu tehlikelerden korumak için bilmeniz gereken temel bilgileri ve pratik önlemleri içermektedir.

SİBER GÜVENLİK: TEMEL KAVRAMLAR

Siber Güvenlik Nedir?

Siber güvenlik, kendimizi, bilgisayarlarımızı, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Basitçe ifade etmek gerekirse, dijital dünyamızı ve içindeki değerli bilgilerimizi korumak için aldığımız önlemlerin tamamıdır.

Neden Önemli?

Uzmanların sık sık vurguladığı gibi, *"Zincir en zayıf halkası kadar güçlüdür. Burada ise en zayıf halka insandır."*. Teknolojik sistemler ne kadar güçlü olursa olsun, kullanıcıların dikkatsizliği veya bilgi eksikliği, siber saldırıların başarılı olmasına neden olabilir.

Siber Güvenlik Tehditleri Kimleri Etkiliyor?

Siber güvenlik tehditleri herkesi etkiler, ancak istatistikler ileri yaştaki bireylerin özellikle hedef alındığını gösteriyor. Son 5 yılda bildirilen şikayetlere göre:

- Toplam şikayet sayısı: 3.79 Milyon
- Toplam maddi kayıp: $37.4 Milyar

Özellikle 60 yaş üstü bireylerin yaşadığı kayıplar diğer yaş gruplarına göre çok daha yüksek seviyelerde seyretmektedir. Bunun nedeni, dolandırıcıların teknolojiye daha az aşina olan kişileri hedef almasıdır.

VERİ İHLALLERİ VE KİŞİSEL VERİ GÜVENLİĞİ

Veri İhlali Nedir?

İşlenen kişisel verilerin yasal olmayan yöntemlerle başkaları tarafından elde edilmesine veri ihlali denilmektedir. 2004-2024 arasında dünya genelinde 107 milyon

138 bin 741 kez kişisel veri ihlali yapıldığı belirtilmiştir. Sadece 2024 yılında 1 milyarın üzerinde kişisel bilgi çalınmıştır.

Türkiye'nin Durumu

Raporlara göre, Türkiye veri sızıntısına en çok maruz kalan 19'uncu ülke konumundadır. (İlk üç sırada: 1. ABD, 2. Rusya, 3. Çin). Son bir yılda veri ihlallerinde %638 artış yaşanmıştır. Bu rakamlar, kişisel veri güvenliğinin ne kadar kritik olduğunu göstermektedir.

ETKİLİ ŞİFRE YÖNETİMİ

Güçlü Şifrelerin Önemi

Dijital dünyada güvenlik, büyük ölçüde şifrelerinizin gücüne bağlıdır. Atalarımız "At ve silah paylaşılmaz" derdi, günümüzde ise "şifre/password paylaşılmaz" diyoruz.
Şifrenizi:
- Başka kişilerle
- Farklı web siteleri arasında paylaşmamak temel kuraldır

Unutmayın: *"Birden fazla kişi bir şey biliyorsa, bu artık bir sır değildir."*

Nasıl Güçlü Şifre Oluşturmalı?

Güçlü bir şifre aşağıdaki özellikleri taşımalıdır:
- En az 12 karakter uzunluğunda olmalı
- Büyük ve küçük harfler içermeli
- Sayılar ve özel karakterler (!,@,#,$,%) barındırmalı
- Tahmin edilebilir bilgiler (doğum tarihi, isim) içermemeli
- Her hesap için farklı şifre kullanılmalı

İstatistiklere göre, internet kullanıcılarının %68'i aynı şifreyi birden fazla hesapta kullanıyor. Bu, bir hesabınız ele geçirildiğinde diğer hesaplarınızın da risk altında olması demektir.

Şifre Yöneticileri

Tüm hesaplarınız için farklı ve karmaşık şifreler oluşturmak ve bunları hatırlamak zor olabilir. Bu sorunu çözmek için:

1. **Tarayıcı Şifre Yöneticileri:** Chrome, Safari ve Edge gibi web tarayıcıları şifrelerinizi güvenli bir şekilde saklayabilir. Bir web sitesine giriş yaptığınızda, tarayıcınız bilgilerinizi kaydetmeyi teklif eder. Kendi kişisel cihazınızda bunu kabul etmeniz güvenlidir.

2. **Şifre Yönetim Uygulamaları:** Daha kapsamlı koruma için özel şifre yönetim uygulamaları kullanabilirsiniz. Bu uygulamalar tüm şifrelerinizi tek bir ana şifre ile korunan güvenli bir kasada saklar.

Önemli: Tarayıcınızın ve işletim sisteminizin her zaman güncel olduğundan emin olun.

İKİ FAKTÖRLÜ DOĞRULAMA (2FA)

İki Faktörlü Doğrulama Nedir?

İki faktörlü doğrulama (2FA), hesaplarınıza ikinci bir koruma katmanı ekleyen güvenlik önlemidir. Şifrenize ek olarak, genellikle telefonunuza gelen tek kullanımlık bir kod ile giriş yapmanızı gerektiriyor.

En yaygın örneği, internet bankacılığı veya online alışverişlerde kullanılan 3D Secure sistemidir. Kredi kartı bilgilerinizi girdikten sonra, telefonunuza gelen kod ile işlemi onaylamanız istenir.

2FA Neleri Önler?

İki faktörlü doğrulama aşağıdaki tehditlere karşı koruma sağlar:

- Şifre çalınması
- Oltalama (phishing) denemeleri
- Sosyal mühendislik saldırıları

- Kuvvetle şifre kırma girişimleri
- Klavye hareketlerinizin kopyalanması
- Diğer şifre hırsızlığı yöntemleri

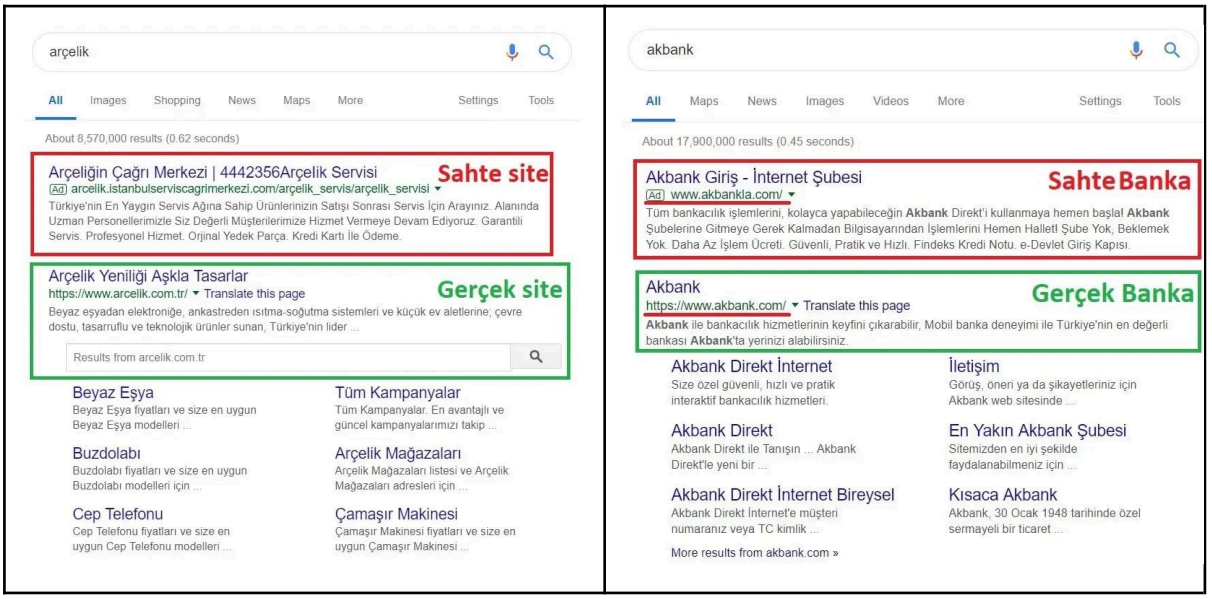
Önemli hesaplarınız (e-posta, bankacılık, sosyal medya) için mutlaka 2FA özelliğini aktifleştirin.

İNTERNETTE GÜVENLİ DOLAŞMA

URL (Web Adresi) Güvenliği

URL (Uniform Resource Locator), bir web sayfasının internet üzerindeki adresidir.
Örneğin: http://www.ege3yas.org.tr
Bir URL şu bileşenlerden oluşur:
- Protokol (http, https)
- Alan adı (www.ege3yas.org)
- Uzantı (.tr)

Güvenli web siteleri "https://" ile başlar ve adres çubuğunda kilit simgesi bulunur. "http://" ile başlayan siteler güvenli değildir ve bu sitelerde kişisel veya finansal bilgilerinizi paylaşmaktan kaçının.



E-posta ve Mesaj Bağlantıları

E-postalarla veya mesajlarla gelen bağlantılara (linklere) tıklamadan önce çok dikkatli olun. Dolandırıcılar, resmi kurumları veya tanıdığınız şirketleri taklit eden sahte e-postalar gönderebilir. Emin olmadığınız durumlarda:

- Bağlantıya tıklamak yerine tarayıcınızda doğrudan ilgili şirketin web sitesini açın
- E-postayı gönderen adresi kontrol edin (örn: info@bankam.com yerine info@bankarn.com gibi benzer ama farklı adresler olabilir)
- Aciliyet uyandıran mesajlara karşı dikkatli olun ("Hesabınız askıya alındı, hemen tıklayın" gibi)

Çerez (Cookie) Güvenliği

Web sitesi ziyaretçilerinin ziyaretleri boyunca bıraktığı verilerin depolandığı küçük dosyalara "çerez (cookie)" denir. Çerezler üç türlüdür:
1. **Fonksiyonel çerezler:** Kullanıcı tercihlerinizi hatırlar ve kolaylık sağlar
2. **Pazarlama çerezleri:** Üçüncü taraflara bilgi iletmek için kullanılır
3. **Zorunlu çerezler:** Web sitesinde gezinmenizi sağlar

Çerezler hakkında en çok tartışılan konu, içerdiği verilerin paylaşımı ve işlenmesiyle ilgili veri sahiplerinden izin alınıp alınmadığıdır. Web sitelerinde karşınıza çıkan "Çerezleri kabul et" mesajlarını okumadan onaylamak yerine, hangi verilerin toplandığını kontrol edin ve gerekirse sadece zorunlu çerezleri kabul edin.

GÜVENLİ ONLİNE ALIŞVERİŞ

Alışveriş Yaparken Dikkat Edilecekler

Online alışveriş yaparken güvende kalmak için şu önlemleri alın:

1. **Güvenilir Siteler Kullanın:** Ucuz/bedava vaatleri olan tanımadığınız sitelerden alışveriş yapmak yerine, bilinen ve güvenilir platformları tercih edin.

2. **3D Secure Kullanın:** 3D Secure (Three Domain Secure), online alışverişlerde kredi kartı veya banka kartı kullanımını daha güvenli hale getiren bir doğrulama sistemidir. Bu sistem, kart sahibinin kimliğini ek bir güvenlik adımıyla doğrulayarak, olası kart dolandırıcılıklarını önlemeyi amaçlar. (Garanti BBVA'nın "3D Secure", İş Bankası'nın "3D Secure", Yapı Kredi'nin "Güvenli İnternet Alışverişi" gibi)

3. **Sanal Kart Kullanın:** Bankalar tarafından sunulan, gerçek kartınızla bağlantılı ama kısıtlı ve geçici limiti olan sanal kartlar kullanın. İşleminiz bittikten sonra kartı kapatabilir veya limitini sıfırlayabilirsiniz.

4. **Kart Bilgilerinizi Kaydetmeyin:** E-ticaret sitelerinin sunduğu "Kredi kartı bilgilerini kaydet" seçeneğini kullanmayın. Her alışverişte bilgilerinizi yeniden girmek zahmetli olabilir, ancak güvenliğiniz için önemlidir.

5. **Online Alışveriş Özelliğini Kullanın:** Bankanızın sunduğu "Kartı online alışverişe aç/kapat" özelliğini kullanın. Alışveriş yapacağınız zaman kartınızı online işlemlere açın ve işleminiz bittikten sonra tekrar kapatın.

CİHAZ GÜVENLİĞİ

Antivirüs Programları

Bilgisayarınızı ve mobil cihazlarınızı kötü amaçlı yazılımlardan korumak için güvenilir antivirüs programları kullanın. Bu programlar:

- Virüsleri tespit eder ve temizler
- Şüpheli web sitelerini engeller
- Kimlik avı denemelerini önler
- Kişisel verilerinizi korur

Güncellemeler

Cihazlarınızdaki işletim sistemini (Windows, macOS, iOS, Android) ve uygulamaları düzenli olarak güncelleyin. Güncellemeler sadece yeni özellikler getirmekle kalmaz, aynı zamanda güvenlik açıklarını da kapatır.

Güncelleme mesajlarını "daha sonra" diyerek ertelemeyin. Bu ertelemeler cihazınızı güvenlik açıklarına karşı savunmasız bırakabilir.

Uygulama Yükleme Güvenliği

Uygulamaları yalnızca resmi uygulama mağazalarından (Apple App Store, Google Play Store) indirin. Bu mağazalar uygulamaları güvenlik açısından kontrol eder ve zararlı yazılımları engellemeye çalışır.

Bilinmeyen kaynaklardan veya güvenli olmayan web sitelerinden uygulama indirmek, cihazınıza kötü amaçlı yazılımlar bulaştırabilir.

Açık WiFi Ağları

Kafeler, havaalanlarında veya diğer halka açık yerlerdeki ücretsiz WiFi ağlarını kullanırken dikkatli olun. Bu ağlar genellikle güvenli değildir ve verileriniz çalınabilir. Açık WiFi ağlarında:

- Online bankacılık işlemleri yapmayın
- Alışveriş yapmayın
- Hassas bilgilerinizi içeren sitelere giriş yapmayın
- Mümkünse VPN (Sanal Özel Ağ) kullanın

VERİ YEDEKLEMENİN ÖNEMİ

Neden Yedekleme Yapmalıyız?

Verilerinizi düzenli olarak yedeklemek, dijital güvenliğinizin önemli bir parçasıdır. Yedekleme şu durumlarda kritik öneme sahiptir:

1. **Donanım arızaları:** Hard disklerin bozulması, SSD'lerin yanması gibi durumlar.
2. **Yazılım hataları:** İşletim sistemi çökmeleri, siber saldırılar, virüs saldırıları veya yanlışlıkla dosya silmeleri.
3. **Doğal afetler:** Yangın, su baskını, deprem gibi olaylar.
4. **Hırsızlık veya kaybolma:** Cihazların çalınması veya kaybolması.

Nasıl Yedekleme Yapılır?

Verilerinizi yedeklemek için birden fazla yöntem kullanabilirsiniz:

- Harici sabit diskler veya USB bellekler
- Bulut depolama hizmetleri (Google Drive, iCloud, OneDrive)
- NAS (Ağa Bağlı Depolama) cihazları

Önemli: 3-2-1 yedekleme kuralını uygulayın: 3 kopya, 2 farklı ortamda, 1 kopya uzak lokasyonda.

YAPAY ZEKA DOLANDIRICILIKLARI

Yeni Nesil Tehditler

Teknoloji geliştikçe dolandırıcılık yöntemleri de gelişiyor. Yapay zeka kullanılarak yapılan dolandırıcılıklar şunları içerir:
1. **Sosyal Mühendislik Planları:**

   - **Kimlik avı (Phishing):** Sahte e-postalar ve web siteleri aracılığıyla kişisel bilgilerinizi çalma girişimleri

   - **Vishing:** Sesli aramalarla yapılan dolandırıcılık
   - **Ticari E-posta dolandırıcılıkları:** İş ortaklarınızı veya yöneticilerinizi taklit eden e-postalar

2. **Şifre Hackleme:** Yapay zeka kullanarak şifre tahmin etme saldırıları

3. **Derin Sahtecilik ve Ses Kopyalama:** Yapay zeka ile üretilen sahte videolar ve ses kayıtları kullanarak tanıdıklarınızı taklit etme

Nasıl Tespit Edebilirsiniz?

Yapay zeka dolandırıcılıklarını tespit etmek giderek zorlaşsa da, hala bazı ipuçları var:

- **Aciliyet:** Dolandırıcılar genellikle hemen harekete geçmeniz için baskı yaparlar. "Acilen para göndermeniz gerekiyor" gibi mesajlar alarm zilleri çaldırmalıdır.

- **Olağandışı istekler:** Birisi sizden beklenmedik bir şekilde para veya hediye kartı göndermenizi veya hassas bilgileri paylaşmanızı isterse dikkatli olun.

- **Garip ifadeler:** Yapay zeka tarafından oluşturulan içerikte hala tuhaf kelime seçimleri veya doğal olmayan dil kullanılabilir.

- **Doğal olmayan ayrıntılar:** Video ve ses kayıtlarında sıradışı arka plan sesleri, garip yüz veya el hareketleri, tutarsız ışıklandırma ve gölgeler ve doğal olmayan hız değişiklikleri gibi şeylere dikkatlice bakın ve dinleyin.

- **Sezgiler:** Etkileşimde bir sorun olduğunu düşünüyorsanız içgüdülerinize güvenin. Bir şey "tuhaf" veya yanlış geliyorsa, muhtemelen öyledir.

Kendinizi Nasıl Koruyabilirsiniz?

1. **Hazırlıklı olun:** Kendinizi ve ailenizi dolandırıcılıklar hakkında eğitin. Beklenmedik bir çağrı, mesaj veya e-posta alırsanız kimlikleri doğrulamak için yalnızca ailenizin bildiği bir kod sözcüğü belirleyin.

2. **Ne paylaştığınıza dikkat edin:** Çevrimiçi olarak hangi kişisel bilgileri paylaştığınız konusunda dikkatli olun. Dolandırıcılar, hayatınızdaki kişisel bilgileri kaldıraç noktası olarak kullanabilir.

3. **Yavaşlayın:** Dolandırıcının yarattığı yanlış aciliyet duygusuna kapılmayın. Eleştirel düşünmek ve sorular sormak için zaman ayırın.

4. **Doğrulayın, doğrulayın, doğrulayın:** Sizinle iletişime geçen kişiyi doğrulamak için güvenilir bir numara veya e-posta adresi kullanın (sizinle iletişime geçen iletişim bilgilerini değil, bildiğiniz ve güvendiğiniz iletişim kanallarını kullanın).

QR KOD DOLANDIRICILIKLARI

QR Kodlarla İlgili Tehlikeler

QR kodlar hayatımızı kolaylaştırırken, aynı zamanda dolandırıcılar için yeni bir yöntem haline geldi. En yaygın QR kod dolandırıcılıkları şunlardır:

1. **Parkmetrelerde QR kod dolandırıcılıkları:** Gerçek QR kodların üzerine yapıştırılan sahte kodlar
2. **Kimlik avı e-postalarında gönderilen sahte QR kodları**
3. **Restoranlarda kurcalanmış QR kodları:** Menü QR kodlarının değiştirilmesi
4. **Postayla gönderilen sahte QR kodları**
5. **Beklenmedik paket teslimatlarında QR kodları**
6. **Sahte COVID-19 test merkezlerinde QR kodları**
7. **Sosyal medya üzerinden gönderilen QR kodları**
8. **Kripto para birimi QR kod dolandırıcılıkları**
9. **Kötü amaçlı yazılım indiren sahte QR kod tarayıcı uygulamaları**

Güvenli QR Kod Kullanımı

QR kodları güvenli bir şekilde kullanmak için:

- Yalnızca güvenilir kaynaklardan gelen QR kodları tarayın

- Bir QR kodu taramadan önce fiziksel olarak kurcalanıp kurcalanmadığını kontrol edin (üzerine başka bir kod yapıştırılmış olabilir)

- QR kodu taradıktan sonra yönlendirildiğiniz URL'yi kontrol edin

- QR kodunu taramak için telefonunuzun kamera uygulamasını kullanın, özel QR kod tarayıcı uygulamaları indirmeyin

MAĞDURİYET DURUMUNDA YAPILMASI GEREKENLER

Eğer bir siber dolandırıcılık veya veri ihlali mağduru olduğunuzu düşünüyorsanız, hemen harekete geçin:

1. İlgili hesapların şifrelerini değiştirin

2. Bankanızı veya kredi kartı şirketinizi bilgilendirin

3. Kredi raporunuzu kontrol edin

4. Kimlik hırsızlığı olasılığına karşı tetikte olun

Resmi Şikayet Kanalları

Çevrimiçi olarak aşağıdaki adresten ihbarda bulunabilirsiniz:
https://onlineislemler.egm.gov.tr

SONUÇ: DİJİTAL AYAK İZİNİZE DİKKAT EDİN

İnternet üzerindeki her hareketimiz bir "dijital ayak izi" bırakır. Bu izler, dolandırıcılar tarafından kullanılabilir. Siber güvenliğin temel ilkesi, dijital ayak izinizi mümkün olduğunca küçük tutmaktır.

Teknoloji hayatımızı kolaylaştırmak için vardır, ancak güvenli kullanmak bizim sorumluluğunuzdadır. Unutmayın ki en iyi teknolojik güvenlik önlemleri bile bilinçli bir kullanıcının yerini tutamaz.

Siber dünyada güvenli kalmak için temel kural: "Doğrula, doğrula, doğrula!".

Siber güvenlik, günümüzün en önemli konularından biridir. Bireylerin, kurumların ve devletlerin dijital varlıklarını korumak için sürekli olarak çaba göstermeleri gerekmektedir. Bilinçli kullanıcı davranışları, güçlü güvenlik önlemleri ve sürekli eğitim, siber tehditlere karşı en etkili savunma yöntemleridir.

Bu rehber, ileri yaştaki internet kullanıcılarını siber dolandırıcılıklara karşı korumak amacıyla hazırlanmıştır. Daha fazla bilgi ve destek için güvenlik uzmanlarına danışabilirsiniz.

Ek Kaynaklar ve Referanslar:

- Sunumu izlemek için: https://doralp.ca
- SİBERAY - Emniyet Genel Müdürlüğü - www.siberay.com
- Tüketicinin Korunması ve Piyasa Gözetimi Genel Müdürlüğü - https://tuketici.ticaret.gov.tr
- KVKK - Kişisel Verileri Koruma Kurumu - www.kvkk.gov.tr
- FBI Internet Crime Complaint Center - https://www.ic3.gov/Home/Index
- National Cyber Security Centre - www.ncsc.gov.uk

Niyazi (Nick) DORALP Kimdir?

1974 Ekim ayında ilk programımı yazdım. TED Ankara Koleji ve Boğaziçi Üniversitesinden mezunum. Hala aynı zevkle ve heyecan ile hem öğreniyorum hem kodluyorum. Yaklaşık 40 yıl Kanada'da yaşadım ve en büyük bankalarının Bilgi İşlem departmanlarında teknik görevlerde yöneticilik yaptım. Bu günlerde sivil toplum kuruluşlarına web siteleri hazırlamak ve iOS (iPhone) ve Android için app geliştiriyorum. 15 adet yazdığım app şu an hem Apple App Store hem Google Play Store da bulunuyor.

Bazı uzmanlık belgelerim:

PMP - Project Management Professional: *Proje Yönetimi Profesyoneli*

CISA - Certified Information Systems Auditor: *Sertifikalı Bilgi Sistemleri Denetçisi*

CFE - Certified Fraud Examiner: *Sertifikalı Dolandırıcılık İnceleme Uzmanı*

EDP - Electronic Document Professional: *Elektronik Belge Profesyoneli*