DIGISENIORBANK

INCLUSIVE DIGITAL BANKING:
EMPOWERING SENIORS WITH DIGITAL SKILLS

2024-1-ES01-KA210-ADU-000243084

TÜRKİYE'DE DİJîtal GÜVENLİK BİLGİLDİRİK

KALİTE İNCELEME TABLOSU

İnceleme	Tarih	Değişikliğin Açıklaması	İmza
0	31/10/2025	Orijinal metin	

Açıklama

Avrupa Birliği tarafından finanse edilmiştir. Burada ifade edilen görüş ve düşünceler yalnızca yazar(lar)a aittir ve Avrupa Birliği'nin veya SEPIE'nin görüş ve düşüncelerini yansıtmayabilir. Ne Avrupa Birliği ne de fonu sağlayan kurum bu görüş ve düşüncelerden sorumlu tutulamaz.

Avrupa Birliği tarafından
ortak finanse edilmektedir

CREATIVE COMMONS LİSANSI

TABLE OF CONTENTS

SLOVENYA'DA DİJİTAL BİLGİ GÜVENLİĞİ

Slovenya'da, kullanıcıları SI-CERT'in (Slovenya Bilgisayar Tehditlerine Müdahale Ekibi) talimatlarına uymaya teşvik ediyoruz; bu ekip, güncel sahte kimlik taklitleri ve dolandırıcı banka mesajları hakkında düzenli olarak uyarılar ve bilgilendirici materyaller yayınlamaktadır.

Buna ek olarak, Slovenya'daki bankalar genellikle SMS veya mobil uygulamalar aracılığıyla iki faktörlü kimlik doğrulama (2FA) kullanmaktadır; kullanıcılara ise güvenli bağlantıları (https://) kontrol ederek ve istenmeyen e-postalar veya SMS mesajlarındaki bağlantılar üzerinden erişimden kaçınarak banka portallarının meşruiyetini doğrulamalarını tavsiye ediyoruz. (SI-CERT, tarihsiz).

1. HÜKÜMET BİLİŞİM GÜVENLİĞİ OFİSİ (GISO)

GISO, Slovenya'nın bilgi güvenliği alanındaki merkezi kurumudur. Siber güvenlik alanındaki ulusal çabaları koordine eder, Bilgi Güvenliği Kanunu'nun (ZInfV) uygulanmasını denetler ve siber güvenlik alanında AB ile işbirliği için ulusal irtibat noktası olarak görev yapar.

GISO, SIGOV-CERT (hükümet sistemleri için) ve SI-CERT (olaylara yönelik daha geniş kapsamlı ulusal müdahale için) gibi kurumlarla yakın işbirliği içindedir. (Gov.si, tarihsiz; Žrt ve Šik Bukovinik, 2021; Gov.si, tarihsiz).

2. SLOVENYA'DA VERİ KORUMA VE SİBER GÜVENLİK YASALARI

Slovenya'nın veri koruma ve siber güvenlikle ilgili yasal çerçevesi şunları içermektedir:

- **Kişisel Verilerin Korunması Kanunu (ZVOP-1):** AB Genel Veri Koruma Yönetmeliği (GDPR) ile uyumludur ve veri koruma ilkelerini ve haklarını tanımlar.
- **Bilgi Güvenliği Kanunu (ZInfV):** Ağ ve bilgi güvenliği ile ilgili AB direktifini uygulamaya koyar; ağ ve bilgi sistemlerinin güvenliğine özel önem verir.
- **Elektronik İletişim Kanunu (ZEKom-1):** Siber güvenlikle ilgili hususlar da dahil olmak üzere elektronik iletişimi düzenler. (Avrupa Komisyonu, 2019; Žrt ve Šik Bukovinik, 2021).

3. KARAR VERİCİLER ARASINDA SİBER GÜVENLİK FARKINDALIĞI

“Zirveye Odaklanmalıyız: Siber ve Bilgi Güvenliği Konusunda Karar Vericilerde Siber Güvenlik Farkındalığıyla İlişkili Faktörler” başlıklı çalışma, Slovenyalı karar vericiler arasında siber güvenlik farkındalığı düzeyini araştırmaktadır.

Hedef odaklı eğitimin ve siber güvenlik uygulamalarını etkileyen örgütsel faktörlerin önemini vurgulamaktadır.

Çalışmanın bazı temel bulguları şunlardır::

- **Belirli tehditler ve çözümler konusunda farkındalığın düşük olması:** Karar vericiler, hizmet reddi (DDoS) saldırıları, botnetler, endüstriyel casusluk ve kimlik sahtekarlığı dahil olmak üzere bazı siber tehditler konusunda sınırlı bir farkındalık sergiledi. Benzer şekilde, güvenlik operasyon merkezleri (SOC), uç nokta algılama ve müdahale (EDR)/genişletilmiş algılama ve müdahale (XDR) yetenekleri, merkezi cihaz yönetimi, çok faktörlü kimlik doğrulama ve kaybolan veya çalınan cihazlarda uzaktan veri silme gibi gelişmiş siber güvenlik çözümleri hakkında da bilgi eksikliği vardı.
- **Örgütsel rolün etkisi:** Siber güvenlik konusundaki farkındalık düzeyi, bireyin kuruluş içindeki rolüne göre farklılık göstermiştir. BT/BS ile ilgisi olmayan üst düzey karar vericiler (örneğin genel müdürler, finans müdürleri), BT/BS yöneticileri ve icracı olmayan yöneticilere kıyasla daha düşük bir farkındalık sergilemiştir..
- **Kişisel özelliklerin etkisi:**
  - **Cinsiyet:** Erkek karar vericiler, genel olarak kadın meslektaşlarına kıyasla siber tehditler ve çözümler konusunda daha fazla farkındalığa sahipti.
  - **Yaş:** Daha yaşlı bireyler genellikle daha yüksek bir farkındalık düzeyine sahipti.
  - **Deneyim:** BT ve bilgi güvenliği alanında daha fazla deneyime sahip olanlar, daha yüksek farkındalık sergiledi.
  - **Eğitim:** Resmi eğitim, siber güvenlik farkındalığı üzerinde önemli bir etki yaratmadı.
  - **Güvenlik önlemleriyle bağlantı:** EDR/XDR yeteneklerine sahip gelişmiş kötü amaçlı yazılım önleme çözümlerini hayata geçiren veya bir SOC kuran kuruluşlarda, siber güvenlik konusunda daha fazla farkındalığa sahip karar vericiler daha sık görülmüştür. (Vrhovec ve Markelj, 2024).

4. ULUSAL SİBER GÜVENLİK STRATEJİSİ

2016 yılının Şubat ayında kabul edilen Slovenya Ulusal Siber Güvenlik Stratejisi, önleme, müdahale ve farkındalık yaratma olmak üzere üç temel unsura dayanmaktadır. Stratejinin amacı, stratejik hedefler, eğitim girişimleri ve siber olaylara yönelik koordineli müdahalelerle sağlam bir ulusal siber güvenlik sistemi kurmaktır (Dig.watch, 2016).

5. SI-CERT: SLOVENYA BİLGİSAYAR YARIŞMA TAKIMI

ARNES (Slovenya Akademik ve Araştırma Ağı) bünyesinde faaliyet gösteren SI-CERT, Slovenya'da siber güvenlik olaylarının ele alınmasından ve siber güvenlik farkındalığının artırılmasından sorumludur. Siber güvenlik sorunlarıyla karşı karşıya kalan hem bireylere hem de kuruluşlara kaynak ve destek sağlamaktadır. (SI-CERT, tarihsiz).

6. EDAVKA VE SI-PASS HAKKINDA BİLGİLENDİRME

Slovenya'daki birçok kullanıcı, dijital kimlik ve vergi hizmetleri için SI-PASS ve eDavki platformlarını kullanmaktadır. Kullanıcılara, sahte saldırıların genellikle bu hizmetlermiş gibi göründüğünü hatırlatmak önemlidir; bu nedenle, e-posta mesajları veya SMS'lerdeki bağlantılar aracılığıyla hiçbir zaman kimlik bilgilerini girmemelidirler. (SI-CERT, tarihsiz).

7. DİJİTAL SERTİFİKALAR (ÖRNEĞİN SIGEN-CA)

Slovenya, dijital imzalar ve güvenli oturum açma işlemleri için SIGEN-CA gibi dijital sertifikaları kullanmaktadır.

Sertifikaların güvenli bir şekilde saklanması, yedeklenmesi ve zamanında yenilenmesi hayati önem taşımaktadır (SI_TRUST, tarihsiz).

8. REKONO

Rekono, Slovenya'nın çevrimiçi kimlik doğrulama ve otentikasyon sistemidir. Kullanıcıların tek bir güvenli hesap kullanarak internet bankacılığı, devlet portalları ve elektronik imza platformları gibi çeşitli dijital hizmetlere güvenli bir şekilde giriş yapmalarına yardımcı olur.

Rekono ile artık farklı hizmetler için ayrı ayrı şifrelere ihtiyacınız yok – çevrimiçi ortamda kimliğinizi doğrulamak için tek bir güvenli yöntem kullanabilirsiniz.

Rekono ne için kullanılır?

- Dijital bankacılık (örn. DH Kişisel) gibi hizmetlere güvenli bir şekilde giriş yapmak için).

- Belgelerin (örneğin sözleşmeler, başvurular) dijital olarak imzalanması için).
- Devletin e-hizmetlerine erişmek için (örn. eDavki, eZPIZ).
- İki faktörlü kimlik doğrulamanın kullanımıacije (npr. SMS or Rekono app code).

Aşağıdakiler dahil olmak üzere çeşitli oturum açma yöntemlerini destekler::

- Kullanıcı adı + şifre.
- Cep telefonunun orijinalliğinin doğrulanması.
- Dijital sertifikalar (SIGEN-CA gibi)).
- Biyometrik doğrulama (mobil uygulama ile) (Rekono, tarihsiz).).

9. MOBİL BANKACILIKTA KİTLE DOĞRULAMA UYGULAMALARININ KULLANIMI

Slovenya'daki bankalar (örn. NLB, Nova KBM, Intesa Sanpaolo), güvenli erişim ve işlem onayları için her bir bankaya özgü uygulamalar (örn. NLB Pay, mBank@Net) kullanmaktadır. Bu uygulamaları yalnızca resmi uygulama mağazalarından indirmeniz ve biyometrik kimlik doğrulama veya PIN kodlarını destekleyen uygulamaları tercih etmeniz çok önemlidir. (NLB, tarihsiz).

10. SI-CERT KAMPANYALARI VE RAPORLAMA ARAÇLARI

SI-CERT, kullanıcıların şüpheli içerikleri bildirebilecekleri varninainternetu.si adlı ulusal portalı yönetmektedir. Bu web sitesi, siber güvenlik konusunda farkındalık yaratmanın yanı sıra dolandırıcılık uyarıları ve sahte tanıtım örnekleri sunmaktadır. (İnternette Güvenli, b. d.).

11. SLOVENYA'DA SON DÖNEMDEKİ EĞİLİMLER (2023–2024)

- Saldırganların banka çalışanları gibi davrandıkları vishing (sesli kimlik hırsızlığı) vakalarındaki artış..
- Slovenya Postası, çevrimiçi bankalar veya vergi dairelerinden gelen sahte SMS'ler.
- Sosyal ağlarda, "hızlı yatırım getirisi" vaat eden ve savunmasız kullanıcıları hedef alan dolandırıcılık vakaları (Štuber, 2025).

İSPANYA'DA DİJİTAL GÜVENLİK BİLGİLERİ

İspanya'da dijital güvenlik konusunda rehberlik hizmeti, INCIBE (Instituto Nacional de Ciberseguridad) tarafından aktif olarak sunulmaktadır. INCIBE, çevrimiçi ortamda zorluklarla karşılaşan bireylere özel kaynaklar ve bir yardım hattı (017) sunmaktadır (INCIBE, tarihsiz). Ayrıca, yaşlılar için öncelikli bir telefonla yardım kanalı oluşturarak, bu gruba özel destekle siber güvenlik endişelerini gidermelerine yardımcı olmaktadır (Tendencias, 2023).

Yaşlı kullanıcılara, özellikle kişisel veya banka bilgilerini isteyen mesajlarda şüpheli bağlantılara tıklamaktan kaçınmaları ve resmi web sitelerine erişmeleri tavsiye edilmektedir. İspanyol bankaları da genellikle SMS kodları veya biyometrik kimlik doğrulama yöntemlerini kullanan güvenli iki aşamalı doğrulama sistemlerine (2FA) güvenmektedir.

1. ULUSAL SİBER GÜVENLİK ENSTİTÜSÜ (INCIBE)

INCIBE (Ulusal Siber Güvenlik Enstitüsü), Dijital Dönüşüm ve Kamu Yönetimi Bakanlığı'na bağlı olarak İspanya'da siber güvenlik alanındaki merkezi otoritedir. Ulusal siber güvenlik stratejilerini koordine eder, vatandaşlara, işletmelere ve hayati öneme sahip operatörlere destek sağlar ve ENISA (Avrupa Birliği Siber Güvenlik Ajansı) gibi Avrupa ağlarıyla irtibat noktası olarak görev yapar.

INCIBE, CCN-CERT (kamu sektörü sistemleri için) gibi kuruluşlarla yakın işbirliği içinde çalışır ve İspanya genelinde tehditleri izleyen ve olay müdahalesini koordine eden CERTSI gibi önemli girişimleri yönetir. Bu kurum, siber güvenliği toplumsal dönüşüm ve inovasyonun itici gücü olarak geliştirmeyi amaçlayan, araştırma, hizmet sunumu ve ilgili paydaşlarla koordinasyona odaklanan bir devlet aracıdır. Ayrıca, vatandaşlar, İspanyol akademik ve araştırma ağı (RedIRIS) ve özellikle stratejik sektörlerdeki işletmeler arasında dijital güveni teşvik etmek için kilit bir kurumdur (INCIBE, tarihsiz).

2. İSPANYA'DA VERİ KORUMA VE SİBER GÜVENLİK YASALARI

İspanya'nın veri koruma ve siber güvenlik konusundaki yasal çerçevesi şunları içermektedir::

- **Veri Koruma ve Dijital Hakların Güvence Altına Alınmasına İlişkin 3/2018 Sayılı Organik Kanun (LOPDGDD):** AB'nin Genel Veri Koruma Yönetmeliği (GDPR) ile uyumlu olup, veri koruma ilkelerini ve bireysel hakları belirler**.**
- **Ulusal Siber Güvenlik Çerçevesi (12/2018 Sayılı Kanun):** AB'nin NIS Direktifini uygulamaya koyar ve ağ ile bilgi sistemlerinin güvenliğine odaklanır.
- **Ulusal Güvenlik Planı (ENS) Hakkında 704/2017 sayılı Kraliyet Kararnamesi:** Kamu sektörü kuruluşları ve kritik altyapı operatörleri içinde bilgi güvenliği için temel çerçeveyi sağlar (Avrupa Komisyonu, 2019; García, 2021)).

3. KARAR VERİCİLER ARASINDA SİBER GÜVENLİK FARKINDALIĞI

Del Real (2025) tarafından yürütülen bir araştırma, İspanya'daki karar vericiler arasında, özellikle teknik bir geçmişi olmayanlar arasında siber güvenlik farkındalığı konusunda endişe verici bir eksiklik olduğunu ortaya koymaktadır. Delphi yöntemi aracılığıyla görüşü alınan uzmanlar, bu farkındalık eksikliğinin dijital ekosistemin etkin yönetimine önemli bir engel teşkil ettiği konusunda hemfikir oldular.

Üst düzey siyasi ve iş dünyası liderleri, siber tehditlerin çok boyutlu doğasını ya da bunların hukuki ve stratejik sonuçlarını genellikle tam olarak kavrayamamaktadır. Buna yanıt olarak çalışma, hedef odaklı eğitim programlarının uygulanmasının ve kurumsal farkındalık çabalarının gelecekte kurulacak bir ulusal siber güvenlik otoritesi bünyesinde merkezileştirilmesinin acil bir ihtiyaç olduğunu vurgulamaktadır. Böyle bir kurum, teknik yetkinlikler ile siyasi karar alma süreçleri arasındaki uçurumu kapatmaya yardımcı olacak ve ortaya çıkan dijital zorluklarla mücadele etmek için daha bilgili ve dayanıklı bir organizasyonel kültürün gelişmesini sağlayacaktır (Del-Real, C. ve Díaz-Fernández, A.M., 2025).

4. ULUSAL SİBER GÜVENLİK STRATEJİSİ

İspanya'nın, ilk olarak 2013 yılında yayımlanan ve 2019 yılında güncellenen bir Ulusal Siber Güvenlik Stratejisi bulunmaktadır. Bu strateji, İspanya'nın bilgi ve telekomünikasyon sistemlerini güvenli bir şekilde kullanmasını sağlamak ve siber tehditlere karşı siber saldırıların önlenmesi, savunulması, tespit edilmesi, bunlara müdahale edilmesi ve toparlanma süreçlerini güçlendirmeyi amaçlamaktadır.

Strateji, beş ana hedefe odaklanmaktadır: siber tehditlere karşı koyma becerilerini geliştirmek, stratejik varlıkların güvenliğini sağlamak, vatandaşlar ve işletmeler için siber güvenliği iyileştirmek, siber suçları soruşturma ve kovuşturma kapasitelerini güçlendirmek ve uluslararası siber güvenlik çabalarına katkıda bulunmak. Ayrıca, tüm sektörlerde farkındalık, eğitim ve en iyi uygulamaları vurgulayan bir siber güvenlik kültürünü teşvik etmektedir (Dig.watch, 2019).

5. INCIBE-CERT: İSPANYA BİLGİSAYAR ACİL DURUM MÜDAHALE EKİBİ

INCIBE-CERT, İspanya'daki vatandaşlar ve özel hukuk tüzel kişilikleri için referans niteliğindeki güvenlik olayı müdahale merkezidir; bu merkez, Ekonomi ve Dijital Dönüşüm Bakanlığı bünyesindeki Dijitalleşme ve Kamu Hizmetleri Devlet Sekreterliği aracılığıyla İspanya Ulusal Siber Güvenlik Enstitüsü (INCIBE) tarafından işletilmektedir (INCIBE-CERT, tarihsiz).

6. CL@VE & VERGİ DAİRESİ FARKINDALIK

İspanya'da pek çok kullanıcı, dijital kimlik ve vergiyle ilgili hizmetler için Cl@ve ve Agencia Tributaria platformlarını kullanmaktadır. Kullanıcılara, kimlik avı saldırılarının sıklıkla bu resmi hizmetleri taklit ettiğini hatırlatmak çok önemlidir; bu nedenle, e-posta veya SMS yoluyla aldıkları bağlantılar üzerinden hiçbir zaman kimlik bilgilerini girmemelidirler (INCIBE, tarihsiz).

7. DİJİTAL SERTİFİKALAR (ÖRNEĞİN, FNMT-RCM)

İspanya, güvenli dijital kimlik doğrulama ve elektronik imzalar için FNMT-RCM (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda) gibi kurumlar tarafından verilen dijital sertifikaları kullanmaktadır. Bu sertifikaların güvenli bir şekilde saklanması, yedeklerinin alınması ve geçerlilik süreleri dolmadan yenilenmelerinin sağlanması büyük önem taşımaktadır (FNMT-RCM, tarihsiz).

8. CL@VE

Cl@ve İspanya'nın resmi çevrimiçi kimlik doğrulama ve otentikasyon sistemidir; tek bir kimlik bilgisi seti kullanılarak çok çeşitli kamu dijital hizmetlerine güvenli erişim sağlamak üzere tasarlanmıştır. Bu sistem, kullanıcıların devlet platformlarına güvenli bir şekilde giriş yapmalarını, belgeleri elektronik olarak imzalamalarını ve kişisel bilgilerine ile idari işlemlere erişmelerini sağlar.

Cl@ve neden kullanılır?

- Agencia Tributaria, DGT ve Sosyal Güvenlik gibi hizmetlere güvenli bir şekilde erişmek için.
- Cl@ve Firma aracılığıyla belgeleri ve başvuruları dijital olarak imzalamak için.
- Birden fazla kamu idaresi web sitesinde kimlik doğrulama işlemini kolaylaştırmak için.
- SMS kodları veya Cl@ve PIN uygulaması gibi iki faktörlü kimlik doğrulama yöntemlerini kullanmak için.

Cl@ve aşağıdakiler dahil olmak üzere çeşitli oturum açma yöntemlerini destekler::

- DNIe (elektronik ulusal kimlik kartı).
- Cl@ve PIN (geçici, SMS tabanlı oturum açma).
- Cl@ve Permanente (şifre + ikinci faktör).
- Dijital sertifikalar (örn., FNMT-RCM).
- Biyometrik kimlik doğrulama (uyumlu mobil cihazlar aracılığıyla) (Cl@ve, tarihsiz).

9. MOBİL BANKA KİMLİK DOĞRULAMA UYGULAMALARI

İspanyol bankaları (örneğin, BBVA, Santander, CaixaBank), güvenli erişim ve işlem onayı için uygulamalar (örneğin, BBVA Wallet, Santander Wallet, CaixaBankNow) kullanmaktadır. Bu uygulamalar, resmi uygulama mağazalarından indirilmeli ve daha yüksek güvenlik için biyometrik kimlik doğrulama veya PIN kodları etkinleştirilmiş olmalıdır.

10. CERT İSPANYA'NIN KAMPANYALARI VE RAPORLAMA ARAÇLARI

CERT İspanya, kullanıcıların şüpheli içerikleri bildirebilecekleri ulusal portal https://www.incibe.es/ciudadania/ayuda/reporte-de-fraude'u işletmektedir. Site, siber güvenlik farkındalığı, dolandırıcılık uyarıları ve kimlik avı örnekleri sunmaktadır (INCIBE, tarihsiz).

11. İSPANYA'DA SON GELİŞMELER (2023–2025)

- **Vishing ve smishing vakalarında artış:** Saldırganlar, kişisel bilgileri çalmak için telefon görüşmeleri veya SMS yoluyla banka çalışanları gibi davranıyor; Zaragoza'da (2025) dikkat çeken olaylar yaşandı (cadenaser.com).
- **Sesli deepfake dolandırıcılığı:** Suçlular, Kanarya Adaları'nda Vodafone'un sanal asistanının kimliğine bürünmek için yapay zeka ile üretilmiş sesler kullandı (2024) (huffingtonpost.es).
- **Çevrimiçi alışveriş dolandırıcılığı:** Bir grup, elektronik eşya satan sahte e-ticaret siteleri oluşturarak 1.000'den fazla kişiyi dolandırdı (2024) (elpais.com).

TÜRKİYE'DE DİJİTAL GÜVENLİK BİLGİLERİ

1. ULUSAL SİBER GÜVENLİK OTORİTELERİ VE YAPISI

Türkiye'de siber güvenlik alanındaki başlıca kamu kurumları şunlardır::

- **USOM (Ulusal Bilgisayar Acil Durum Müdahale Merkezi):** Ulaştırma ve Altyapı Bakanlığı bünyesinde faaliyet gösteren USOM, kamu kurumlarını, kritik altyapıyı ve vatandaşları etkileyen siber güvenlik olaylarını izler, analiz eder ve bunlara müdahale eder. Ayrıca farkındalık kampanyaları da yürütür.
- **BTK (Bilgi ve İletişim Teknolojileri Kurumu):** Telekomünikasyon ve internet trafiğinin düzenlenmesinden sorumlu olan BTK, aynı zamanda e-imza, elektronik iletişim güvenliği ve kişisel verilerin korunması ile ilgili teknik denetimleri de yürütür.
- **TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü:** Güvenlik altyapıları ve yerli siber güvenlik yazılımları geliştirir; kamu kurumları için eğitim ve araştırma faaliyetleri yürütür.
- **Public-CERT:** Kamu kurumlarının dijital sistemlerini hedef alan tehditleri önlemek amacıyla kurulan bu birim, kurum içi Siber Olay Müdahale Ekiplerini (SOME) koordine eder.

2. HUKUKİ VE MEVZUAT ÇERÇEVESİ

Türkiye'de dijital güvenlikle ilgili başlıca yasa ve yönetmelikler:

- **Kişisel Verilerin Korunması Kanunu (KVKK, 2016)**: AB'nin GDPR'sine benzer şekilde, bu kanun kişisel verilerin işlenmesi, saklanması ve aktarılmasına ilişkin standartları belirler. Kişisel Verileri Koruma Kurumu, bu alandaki düzenleyici kurumdur.
- **Elektronik İmza Kanunu (2004)**: Dijital belgelerin ve işlemlerin hukuki geçerliliğini sağlamak amacıyla elektronik imzaların kullanımını düzenler.
- **5651 Sayılı Kanun**: İnternet üzerinden erişilen içeriği, trafik verilerinin saklanmasını ve erişim kısıtlamalarını düzenler.
- **Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023):** Kritik altyapıyı korumayı, SOME ağını genişletmeyi ve siber tehditlere karşı farkındalığı ve kapasiteyi artırmayı amaçlamaktadır.

3. DİJİTAL KİMLİK VE E-YÖNETİM UYGULAMALARI

- **e-Devlet Portalı (turkiye.gov.tr):** Vatandaşlara dijital hizmetler sunan merkezi bir platformdur. Kimlik doğrulama yöntemleri arasında e-imza, mobil imza, SMS ile doğrulama veya internet bankacılığı entegrasyonu yer almaktadır.

- **Elektronik Kimlik Kartı**: Dijital imza ve kimlik doğrulamasına olanak tanıyan akıllı kimlik kartları.
- **MERNIS ve Kimlik Paylaşım Sistemi**: Resmi kurumlar arasında güvenli kimlik doğrulama ve veri alışverişi için gerekli altyapı.

4. CYBERSECURITY PRACTICES IN BANKING

- **Türkiye'deki tüm bankalar, iki faktörlü kimlik doğrulamayı (2FA)** zorunlu hale getirmiştir. Müşteriler, internet bankacılığı işlemleri sırasında SMS ile tek kullanımlık şifre (OTP), mobil uygulamalar üzerinden push bildirimleri, parmak izi veya yüz tanıma yöntemlerini kullanmaktadır.
- **BRSA (Bankacılık Düzenleme ve Denetleme Kurumu),** "Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Yönetmeliği" kapsamında sektörü denetlemektedir.
- **Mobil Güvenlik Uygulamaları:** Ziraat Mobile, İşCep ve Garanti BBVA Mobile gibi bankalara özel uygulamalar, biyometrik kimlik doğrulama, ekran kilidi, şifreleme ve sahte uygulama uyarıları gibi özellikler sunar.

5. FARKINDALIK VE EĞİTİM KAMPANYALARI

1. **Siberay (https://siberay.com.tr):** BTK tarafından işletilen, dijital okuryazarlık, güvenli internet kullanımı, çocuk eğitim içerikleri ve dolandırıcılık uyarıları sunan bir siber güvenlik farkındalık platformu.
2. **KVKK Eğitim Programları:** Kişisel veri koruma üzerine e-öğrenme modülleri ve halka açık seminerler.

- **USOM Uyarıları ve Raporları:** Oltalama, kötü amaçlı yazılım ve fidye yazılımı tehditleriyle ilgili kamuya açık uyarılar ve vaka çalışmaları.

6. TÜRKIYE'DE SIBER TEHDIT EĞILIMLERI (2023–2024)

1. **Sahte Banka SMS'leri ve Aramaları (Vishing):** Banka temsilcisi kimliğini sokan kişilerin yer aldığı dolandırıcılıklar artıyor.
2. **Sosyal Medya Üzerinden Yatırım Dolandırıcılıkları:** Kripto veya hisse senedi ticareti yoluyla hızlı zenginlik vaat eden sahte reklamlar.

- **Deepfake ve Phishing:** Yüz tanıma sistemlerinin, sahte kimlik belgelerinin ve sosyal mühendislik saldırılarının manipülasyonu.

7. DIJITAL SERTIFIKALAR VE GÜVENLI GIRIŞ SISTEMLERI

- **E-imza ve Mobil İmza:** Kamu SM (Kamu Sertifikasyon Merkezi) tarafından verilir, e-Hükümet, e-Fatura ve e-Bildirim için kullanılır.
- **KEP (Kayıtlı Elektronik Posta):** Güvenli belge iletimi için gerekli olan yasal olarak geçerli bir dijital yazışma sistemi.
- **Türkiye Kartı ve Birleşik Giriş Sistemleri:** Tek bir kimlik ile çeşitli kamu hizmetlerine güvenli erişim sağlamak için devam eden çalışmalar.

8. KURUMSAL GÜVENLIK STANDARTLARI VE DENETIMLER

- ISO/IEC 27001 bilgi güvenliği yönetim sistemi, birçok büyük kamu ve özel kurum tarafından uygulanmaktadır.
- USOM ve BTK, kamu kurumlarında ve kritik altyapı operatörlerinde denetimler yapar ve güvenlik açıklıklarını bildirir.

9. SIBER GÜVENLIKTE ULUSLARARASI IŞ BIRLIĞI

- Türkiye, bilgi paylaşımı, standart uyumlaştırma ve ortak tatbikatlar konusunda Avrupa Birliği Siber Güvenlik Ajansı (ENISA) ile iş birliği yapmaktadır.
- NATO CCDCOE (İşbirlikçi Siber Savunma Mükemmeliyet Merkezi) etkinliklerine gözlemci olarak katılır.
- Türk Devletleri Örgütü, bölgesel siber güvenlik iş birliği stratejileri geliştirir.

BIBLIYOGRAFYA

Dig.watch (2016, February). *Slovenian National Cyber Security Strategy.* Available on April 18 2025 through:

→ https://dig.watch/resource/slovenian-national-cyber-security-strategy?utm_source=chatgpt.com

European Commission (2019). *Digital Government Factsheet 2019*:

→ chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf

Gov.si. (n. d.). *About the Government Information Security Office.* Available on April 22 2025 through:

→ https://www.gov.si/en/state-authorities/government-offices/government-information-security-office/about-the-office/?utm_source=chatgpt.com

Gov.si (n. d.b). *Information and Cyber Security Division.* Available on April 22 2025 through:

→ https://www.gov.si/en/state-authorities/government-offices/government-information-security-office/about-the-office/information-and-cyber-security-division/?utm_source=chatgpt.com

NLB. (n. d.). *Tips on security measures when using the NLB service Click "E-BANKING".* Available on April 22 2025 through:

→ https://nlb-kos.com/en/news/16/keshilla-mbi-masat-e-sigurise-ne-perdorimin-e-sherbimit-nlb-klik-e-banking

Rekono. (n. d.). *O nas.* Available on April 19 2025 through:

→ https://www.rekono.si/splosno/

SI-CERT. (n. d.). *About SI-CERT.* Available on April 17 2025 through:

→ https://www.cert.si/en/about-si-cert/

SI-TRUST. (n. d.). *Digitalna potrdila in mobilna identiteta.* Available on April 22 2025 through:

→ https://www.si-trust.gov.si/

Štuber, C. (2025, April 12). Spletne prevare: Zmožnosti tehnologije globokega ponarejanja (deep fake). *RTV SLO*:

→ https://www.rtvslo.si/znanost-in-tehnologija/spletne-prevare-zmoznosti-tehnologije-globokega-ponarejanja-deep-fake/742451

Varni na internet. (n. d.). *Najpogostejše težave, s katerimi se soočajo spletni uporabniki.* Available on April 22 2025 through:

→ https://www.varninainternetu.si/

Vrhovec, S. Markelj, B. (2024, April 6). *We needto aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers*:

→ chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://arxiv.org/pdf/2404.04725

Žrt, A. Šik Bukovnik, I. (2021, March 5). Data protection and cybersecurity laws in Slovenia. *CMS Law*:

→ https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/slovenia?utm_source=chatgpt.com

Banco de España (2020). *Mobile banking security and recommendations*:

→ https://www.bde.es

Cadenaser (2025). *Seis detenidos en Zaragoza por estafar más de 100,000 euros a 53 personas*:

→ https://cadenaser.com

Del-Real, C., & Díaz-Fernández, A. M. (2025). *Who will govern cybersecurity in Spain by 2035? Results from a Delphi study.* Futures & Foresight Science, 7, e208:

→ https://doi.org/10.1002/ffo2.208

Dig.watch (2019, April). *Spain's National Cybersecurity Strategy*:

→ https://dig.watch/resource/spains-national-cybersecurity-strategy

El País (2024). *Una red criminal estafó cinco millones a más de 1,000 víctimas en ventas en línea de tecnología de alta gama*:

→ https://elpais.com

European Commission (2019). *Digital Government Factsheet 2019 Spain*:

→ https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Spain_2019_1.pdf

FNMT-RCM. (n.d.). *Certificados digitales. Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda*:

→ https://www.sede.fnmt.gob.es/certificados

García, J. (2021). *La Estrategia de Seguridad Nacional 2021 y la National Security Strategy 2022: una visión compartida.* Dialnet:

→ https://dialnet.unirioja.es/servlet/articulo?codigo=9049920

Gobierno de España (n.d.). *Sistema Cl@ve*:

→ https://clave.gob.es

Huffingtonpost (2024). *La estafa Vodafone comenzada en Canarias*:

→ https://www.huffingtonpost.es

INCIBE (n.d.-a). *Consejos de ciberseguridad para ciudadanos. Instituto Nacional de Ciberseguridad*:

→ https://www.incibe.es

INCIBE (n.d.-b). *Cybersecurity and reporting tools. Instituto Nacional de Ciberseguridad*:

→ https://www.incibe.es

Trendencias (2023). *Cómo actuar ante las ciberestafas: el teléfono 017 de INCIBE abre un canal prioritario para personas mayores*:

→ https://www.trendencias.com/silver/como-actuar-ciberestafas-telefono-017-incibe-abre-canal-prioritario-para-personas-mayores

BTK:

→ https://www.btk.gov.tr

USOM:

→ https://www.usom.gov.tr

Siberay Platform:

→ https://www.siberay.com.tr

Kamu SM:

→ https://www.kamusm.gov.tr

KVKK:

→ https://www.kvkk.gov.tr

BDDK:

→ https://www.bddk.org.tr

e-Government:

→ https://www.turkiye.gov.tr

National Cybersecurity Strategy and Action Plan 2020–2023

Cyber Threat Reports (BTK & USOM)

Bu belge bunu geliştirmiştir...

KONSORSIYUM

BAŞ ORTAK

HORIZONTE XXII (İspanya)

ORTAKLAR

LJUDSKA UNIVERZA, ZAVOD ZA IZOBRAŽEVANJE IN KULTURO, ROGAŠKA SLATINA (Slovenya)

EGESTIONPYME INTERNET S.L. (İspanya)

KULTUR EGITIM VE PROJE DERNEGI – KEPDER (Türkiye)