DIGISENIORBANK

INCLUSIVE DIGITAL BANKING: EMPOWERING SENIORS WITH DIGITAL SKILLS

2024-1-ES01-KA210-ADU-000243084

DIGITAL SECURITY INFORMATION

QUALITY REVIEW TABLE

Review	Date	Description of the Modification	Signature
0	29/08/2025	Original wording	

DISCLAIMER

Co-funded by the European Union. The opinions and points of view expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union nor the granting authority can be held responsible for them.

CREATIVE COMMONS LICENCE

TABLE OF CONTENTS

DIGITAL SECURITY INFORMATION IN SLOVENIA

In Slovenia, users are encouraged to follow guidance provided by SI-CERT (Slovenian Computer Emergency Response Team), which regularly publishes alerts and educational material about current phishing schemes and fraudulent banking messages.

Additionally, banks in Slovenia commonly use two-factor authentication (2FA) via SMS or mobile apps, and users are advised to verify the legitimacy of banking portals by checking for secure connections (https://) and avoiding access via links in unsolicited emails or SMS messages (SI-CERT, n. d.).

1. GOVERNMENT INFORMATION SECURITY OFFICE (GISO)

GISO is Slovenia's central authority for information security. It coordinates national cybersecurity efforts, oversees the implementation of the Information Security Act (ZInfV), and serves as the national point of contact for EU cybersecurity cooperation.

GISO works closely with entities like SIGOV-CERT (for government systems) and SI-CERT (for broader national incident response) (Gov.si, n. da.; Žrt and Šik Bukovinik, 2021; Gov.si, n. d.b).

2. DATA PROTECTION AND CYBERSECURITY LAWS IN SLOVENIA

Slovenia's legal framework for data protection and cybersecurity includes:

- **Personal Data Protection Act (ZVOP-1):** Aligns with the EU's GDPR, outlining data protection principles and rights.
- **Information Security Act (ZInfV):** Implements the EU's NIS Directive, focusing on the security of network and information systems.
- **Electronic Communications Act (ZEKom-1):** Regulates electronic communications, including aspects related to cybersecurity. (European Commission, 2019; Žrt and Šik Bukovinik, 2021).

3. CYBERSECURITY AWARENESS AMONG DECISION-MAKERS

A study titled "We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers" explores the cybersecurity awareness levels among Slovenian decision-makers.

It highlights the importance of targeted training and organizational factors influencing cybersecurity practices.

Some key findings from the study are:

- **Low Awareness of Specific Threats and Solutions:** Decision-makers exhibited limited awareness of certain cyber threats, including distributed denial-of-service (DDoS) attacks, botnets, industrial espionage, and phishing. Similarly, there was a lack of familiarity with advanced cybersecurity solutions such as Security Operation Centers (SOC), endpoint detection and response (EDR)/extended detection and response (XDR) capabilities, centralized device management, multi-factor authentication, and remote data deletion on lost or stolen devices.
- **Impact of Organizational Role:** The level of cybersecurity awareness varied based on the individual's role within the organization. Non-IT/IS executive decision-makers (e.g., CEOs, CFOs) demonstrated lower awareness compared to IT/IS executives and non-executive roles.
- **Influence of Personal Characteristics:**
  - **Gender:** Male decision-makers were generally more aware of cybersecurity threats and solutions than their female counterparts.
  - **Age:** Older individuals tended to have higher awareness levels.
  - **Experience:** Those with more experience in IT and information security showed greater awareness.
  - **Education:** Formal education level did not significantly impact cybersecurity awareness.
  - **Association with Security Measures:** Organizations that had adopted advanced antimalware solutions with EDR/XDR capabilities or established a SOC were more likely to have decision-makers with higher cybersecurity awareness (Vrhovec and Markelj, 2024).

4. NATIONAL CYBERSECURITY STRATEGY

Slovenia's National Cybersecurity Strategy, adopted in February 2016, is built on three pillars: prevention, response, and awareness. It aims to establish a robust national cybersecurity system through strategic goals, education initiatives, and coordinated responses to cyber incidents (Dig.watch, 2016).

5. SI-CERT: SLOVENIAN COMPUTER EMERGENCY RESPONSE TEAM

SI-CERT, operating under ARNES (Academic and Research Network of Slovenia), is responsible for handling cybersecurity incidents and promoting cybersecurity awareness in Slovenia. It provides resources and support for both individuals and organizations facing cybersecurity challenges (SI-CERT, n. d.).

6. EDAVKI & SI-PASS AWARENESS

Many users in Slovenia use SI-PASS and eDavki platforms for digital identity and tax services. It's important to remind users that phishing attacks often impersonate these services, so they should never enter credentials via links from emails or SMS (SI-CERT, n. d.).

7. DIGITAL CERTIFICATES (E.G., SIGEN-CA)

Slovenia uses digital certificates like SIGEN-CA for digital signatures and secure login.

It's critical to keep certificates safe, back them up, and renew them timely. (SI_TRUST, n. d.)

8. REKONO

Rekono is a Slovenian online identification and authentication system. It helps users safely log in to various digital services, such as online banking, government portals, and e-signature platforms, using a single secure account.

With Rekono, you do not need multiple passwords for different services — you can use one secure method to prove your identity online.

Why is Rekono used?

- To safely log in to services like digital banking (e.g., DH Osebni).
- To digitally sign documents (e.g., contracts, applications).
- To access government e-services (e.g., eDavki, eZPIZ).
- To use two-factor authentication (e.g., SMS or Rekono app code).

It supports various login methods, including:

- Username + password.
- Mobile phone authentication.

- Digital certificates (like SIGEN-CA).
- Biometric verification (with mobile app) (Rekono, n. d.).

9. USE OF MOBILE BANK AUTHENTICATION APPS

Slovenian banks (e.g., NLB, Nova KBM, Intesa Sanpaolo) use bank-specific apps (e.g., NLB Pay, mBank@Net) for secure access and transaction approval. It is very important that they are download only from official app stores and enable biometrics or PINs (NLB, n. d.).

10. SI-CERT CAMPAIGNS AND REPORTING TOOLS

SI-CERT runs the national portal varninainternetu.si, where users can report suspicious content. The site offers cybersecurity awareness, scam alerts, and phishing examples (Varni na internetu, n. d.).

11. RECENT TRENDS IN SLOVENIA (2023–2024)

- Rise in vishing (voice phishing) where attackers pretend to be bank staff.
- Fake SMS from Pošta Slovenije, online banks, or tax services.
- Social media scams offering “quick investment returns” targeting vulnerable users (Štuber, 2025).

DIGITAL SECURITY INFORMATION IN SPAIN

In Spain, digital security guidance is actively provided by INCIBE (Instituto Nacional de Ciberseguridad), which offers dedicated resources and a helpline (017) for individuals who face difficulties online (INCIBE, n.d). It has also created a priority telephone assistance channel for older adults, helping them address cybersecurity concerns with tailored support (Tendencias, 2023).

Older users are advised to avoid clicking on suspicious links, especially in messages that ask for personal or banking data, and to access official websites. Spanish banks also rely on secure two-step verification systems (2FA), often using SMS codes or biometric identification.

1. NATIONAL CYBERSECURITY INSTITUTE (INCIBE)

INCIBE (National Cybersecurity Institute) is the central authority on cybersecurity in Spain, under the Ministry for Digital Transformation and Public Administration. It coordinates national cybersecurity strategies, provides support to citizens, businesses, and essential operators, and serves as a point of contact with European networks such as ENISA (European Union Agency for Cybersecurity).

INCIBE works closely with organizations like CCN-CERT (for public sector systems) and manages key initiatives such as CERTSI, which monitors threats and coordinates incident response across Spain. It is a government tool aimed at developing cybersecurity as a driver for social transformation and innovation, focusing on research, service provision, and coordination with relevant stakeholders. It is also a key entity for promoting digital trust across citizens, the Spanish academic and research network (RedIRIS), and businesses, particularly in strategic sectors (INCIBE, n.d).

2. DATA PROTECTION AND CYBERSECURITY LAWS IN SPAIN

Spain's legal framework for data protection and cybersecurity includes:

- **Organic Law 3/2018 on Data Protection and Guarantee of Digital Rights (LOPDGDD):** Aligns with the EU's General Data Protection Regulation (GDPR), establishing data protection principles and individual rights.
- **National Cybersecurity Framework (Ley 12/2018):** Implements the EU's NIS Directive, focusing on the security of network and information systems.
- **Royal Decree 704/2017 on the National Security Scheme (ENS):** Provides the baseline for information security within public sector organizations and critical infrastructure operators (European Commission, 2019; García, 2021).

3. CYBERSECURITY AWARENESS AMONG DECISION-MAKERS

A study conducted by Del Real (2025) shows a concerning gap in cybersecurity awareness identified among decision-makers in Spain, particularly those without a technical background. Through the Delphi method, the consulted experts agreed that this lack of awareness poses a significant barrier to effective governance of the digital ecosystem.

High-level political and business leaders often fail to fully grasp the multidimensional nature of cyber threats or their legal and strategic implications. As a response, the study emphasizes the urgent need to implement targeted training programs and centralize institutional awareness efforts within a future national cybersecurity authority. Such an entity would help bridge the gap between technical capabilities and political decision-making, fostering a more informed and resilient organizational culture to confront emerging digital challenges (Del-Real, C. and Díaz-Fernández, A.M., 2025).

4. NATIONAL CYBERSECURITY STRATEGY

Spain has a National Cybersecurity Strategy that was first published in 2013 and updated in 2019. The strategy aims to ensure that Spain makes secure use of information and telecommunications systems and strengthens cyber-attack prevention, defence, detection, response, and recovery actions against cyber threats.

The strategy focuses on five main goals: enhancing skills to counter cyber threats, ensuring the security of strategic assets, improving cybersecurity for citizens and businesses, strengthening capabilities to investigate and prosecute cybercrimes, and contributing to international cybersecurity efforts. It also promotes a cybersecurity culture emphasizing awareness, education, and best practices across all sectors (Dig.watch, 2019).

5. INCIBE-CERT: SPANISH COMPUTER EMERGENCY RESPONSE TEAM

INCIBE-CERT is the reference security incident response center for citizens and private law entities in Spain, operated by The Spanish National Cybersecurity Institute (INCIBE), under the Ministry of Economy Affairs and Digital Transformation, through the Secretary of State for Digitalisation and Public Service (INCIBE-CERT, n.d).

6. CL@VE & AGENCIA TRIBUTARIA AWARENESS

In Spain, many users rely on Cl@ve and the Agencia Tributaria platforms for digital identity and tax-related services. It is essential to remind users that phishing attacks frequently mimic these official services, so they should never enter their credentials through links received via email or SMS (INCIBE, n.d).

7. DIGITAL CERTIFICATES (E.G., FNMT-RCM)

Spain uses digital certificates issued by entities like the FNMT-RCM (Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda) for secure digital identification and electronic signatures. It is essential to store these certificates securely, keep backups, and ensure they are renewed before expiration (FNMT-RCM, n.d.).

8. CL@VE

Cl@ve is Spain’s official online identification and authentication system, designed to provide secure access to a wide range of public digital services using a single set of credentials. It allows users to log in safely to government platforms, sign documents electronically, and access personal information and administrative procedures.

Why is Cl@ve used?

- To securely access services like the Agencia Tributaria, DGT, and Social Security.
- To digitally sign documents and applications via Cl@ve Firma.
- To simplify authentication across multiple public administration websites.
- To use two-factor authentication methods, such as SMS codes or the Cl@ve PIN app.

Cl@ve supports various login methods, including:

- DNIe (electronic national ID).
- Cl@ve PIN (temporary, SMS-based login).
- Cl@ve Permanente (password + second factor).
- Digital certificates (e.g., FNMT-RCM).
- Biometric identification (via compatible mobile devices) (Cl@ve, n.d.).

9. MOBILE BANK AUTHENTICATION APPS

Spanish banks (e.g., BBVA, Santander, CaixaBank) use apps (e.g., BBVA Wallet, Santander Wallet, CaixaBankNow) for secure access and transaction approval. These apps must be downloaded from official stores and have biometrics or PINs enabled for enhanced security.

10. CERT SPAIN CAMPAIGNS AND REPORTING TOOLS

CERT Spain operates the national portal https://www.incibe.es/ciudadania/ayuda/reporte-de-fraude, where users can report suspicious content. The site provides cybersecurity awareness, scam alerts, and phishing examples (INCIBE, n.d.).

11. RECENT TRENDS IN SPAIN (2023–2025)

- **Rise in vishing and smishing:** Attackers impersonate bank staff via phone calls or SMS to steal personal information, with notable incidents in Zaragoza (2025) (cadenaser.com).
- **Voice deep fake scams:** Criminals used AI-generated voices to impersonate Vodafone's virtual assistant in the Canary Islands (2024) (huffingtonpost.es).
- **Online shopping fraud:** A group defrauded over 1,000 victims by creating fake e-commerce sites selling electronics (2024) (elpais.com).

DIGITAL SECURITY INFORMATION IN TÜRKİYE

1. NATIONAL CYBERSECURITY AUTHORITIES AND STRUCTURE

The main public authorities in the field of cybersecurity in Türkiye are:

- **USOM (National Computer Emergency Response Centre):** Operating under the Ministry of Transport and Infrastructure, USOM monitors, analyses, and responds to cybersecurity incidents affecting public institutions, critical infrastructure, and citizens. It also conducts awareness campaigns.
- **BTK (Information and Communication Technologies Authority):** Responsible for regulating telecommunications and internet traffic, BTK also oversees technical inspections related to e-signature, electronic communications security, and personal data protection.
- **TÜBİTAK BİLGEM Cybersecurity Institute:** Develops security infrastructures, domestic cybersecurity software, and conducts training and research for public institutions.
- **Public-CERT:** Established to prevent threats targeting digital systems of public institutions, this unit coordinates internal Cyber Incident Response Teams (SOMEs).

2. LEGAL AND REGULATORY FRAMEWORK

Key laws and regulations related to digital security in Türkiye:

- **Personal Data Protection Law (KVKK, 2016):** Similar to the EU's GDPR, this law sets standards for the processing, storage, and transfer of personal data. The Personal Data Protection Authority is the regulatory body.
- **Electronic Signature Law (2004):** Regulates the use of electronic signatures to ensure legal validity of digital documents and transactions.
- **Law No. 5651:** Regulates content accessed via the internet, traffic data retention, and access restrictions.
- **National Cybersecurity Strategy and Action Plan (2020–2023):** Aims to protect critical infrastructure, expand the SOME network, and raise awareness and capacity against cyber threats.

3. DIGITAL IDENTITY AND E-GOVERNMENT APPLICATIONS

- **e-Government Gateway (turkiye.gov.tr):** Central platform offering digital services to citizens. Authentication methods include e-signature, mobile signature, SMS verification, or online banking integration.
- **Electronic Identity Card:** Smart ID cards enabling digital signature and identity verification.
- **MERNIS & Identity Sharing System:** Infrastructure for secure identity verification and data exchange among official institutions.

4. CYBERSECURITY PRACTICES IN BANKING

- **All banks in Türkiye have made two-factor authentication (2FA) mandatory.** Customers use SMS OTP, push notifications via mobile apps, fingerprint, or facial recognition during online banking transactions
- **BRSA (Banking Regulation and Supervision Agency)** supervises the sector under the 'Regulation on Information Systems and Electronic Banking Services.
- **Mobile Security Apps:** Bank-specific apps such as Ziraat Mobile, İşCep, and Garanti BBVA Mobile offer biometric authentication, screen lock, encryption, and fake app warnings.

5. AWARENESS AND EDUCATION CAMPAIGNS

- **Siberay (https://siberay.com.tr):** A cybersecurity awareness platform run by BTK, offering digital literacy, safe internet use, children's education content, and scam alerts.
- **KVKK Training Programs:** E-learning modules and public seminars on personal data protection.
- **USOM Alerts and Reports:** Public warnings and case studies about phishing, malware, and ransomware threats.

6. CYBER THREAT TRENDS IN TÜRKIYE (2023–2024)

- **Fake Bank SMS and Calls (Vishing):** Increased scams involving individuals impersonating bank representatives.

- **Investment Scams via Social Media:** Fraudulent ads promising quick riches through crypto or stock trading.
- **Deepfake and Phishing:** Manipulation of facial recognition systems, fake identity documents, and social engineering attacks.

7. DIGITAL CERTIFICATES AND SECURE LOGIN SYSTEMS

- **E-signature & Mobile Signature:** Issued by Kamu SM (Public Certification Center), used for e-Government, e-Invoice, and e-Notification.
- **KEP (Registered Electronic Mail):** A legally valid digital correspondence system required for secure document transmission.
- **Türkiye Card & Unified Login Systems:** Ongoing efforts to enable secure access to various public services with a single ID.

8. INSTITUTIONAL SECURITY STANDARDS AND AUDITS

- ISO/IEC 27001 information security management system is implemented by many large public and private institutions.
- USOM and BTK conduct audits and report vulnerabilities in public institutions and critical infrastructure operators.

9. INTERNATIONAL COOPERATION IN CYBERSECURITY

- Türkiye cooperates with the European Union Agency for Cybersecurity (ENISA) on information sharing, standard harmonization, and joint exercises.
- Participates as an observer in NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) events.
- The Organization of Turkic States develops regional cybersecurity cooperation strategies.

BIBLIOGRAPHY

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)

This document has been developed by this…

CONSORTIUM

LEADER

HORIZONTE XXII (Spain)

PARTNERS

LJUDSKA UNIVERZA, ZAVOD ZA IZOBRAZEVANJE IN KULTURO, ROGASKA SLATINA (Slovenia)

EGESTIONPYME INTERNET S.L. (Spain)

KULTUR EGITIM VE PROJE DERNEGI – KEPDER (Türkiye)