I.D. RISK ALERTS

Open Source Edition

Identity and Biometric Vulnerabilities | Threats and Risks | Mitigations

Welcome

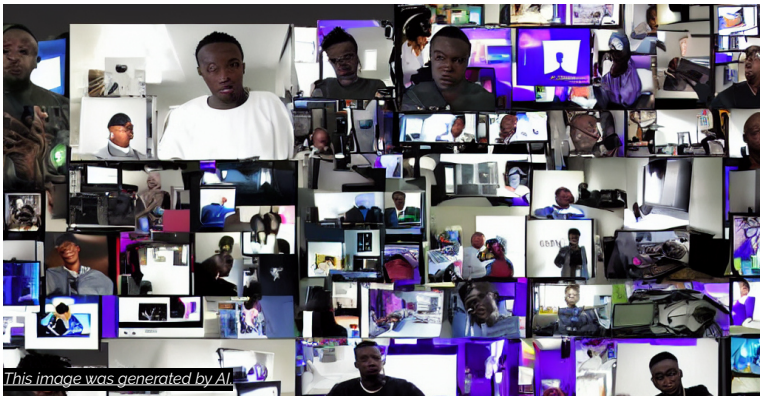
The I.D. Risk Alerts newsletter (open source edition) is a quarterly newsletter with analysis on recent ID fraud, biometric threats and identity vulnerabilities that are already known in the public domain. A comprehensive bi-annual report will also be available to select BixeLab subscribers.

Belgium's Digital Identity Wallet Launch and EU's eIDAS Framework

Belgium has become one of the first countries in European Union to launch a national digital identity wallet, MyGov.be, following the EU's eIDAS 2.0 regulation. Meanwhile, the European Union continues to push its digital identity wallet initiative, guided by the EU Digital Identity Architecture Reference Framework(ARF) v1.0.0 to ensure security, privacy, and user control. Additionally, the European Data Protection Board's "Opinion 11/2024" highlights that centralised storage models are incompatible with General Data Protection Regulation (GDPR) unless additional protective measures are applied, even as biometric technologies continue to be adopted across Europe, with Spain recently launching facial recognition scanners supported by the EU Commission pilot programs.

Increasing Use of Surveillance Technology and Concerns About Privacy and Rights

Recent worldwide developments indicate a surge in the deployment of surveillance technologies worldwide, raising privacy and human rights concerns. In Germany, the police have adopted high-definition cameras and live facial recognition technology in Berlin and Saxony, aimed at catching suspects; however, critics and legal experts have expressed concerns about privacy infringements. In parallel, Mexico's popular tourist destination of Cozumel has implemented an advanced surveillance system with facial recognition and license plate reading capabilities to enhance security. Meanwhile, Belarus has expanded its video surveillance system with over 35,000 cameras incorporating facial recognition amidst rising political repression.



Advanced Romance Scams via Real-Time Face-Swapping by Cybercriminals in Nigeria

Modality: **Face** Attack Instrument: **Real-time face-swapping, deepfake technology** Location: **Nigeria** Date of report: **April 2024**

The "Yahoo Boys" scam, an elaborate form of catfishing using real-time face-swapping technology, has emerged. This scheme involves sophisticated cybercriminals, primarily based in Nigeria, who deceive victims by impersonating lovers over video calls. Utilising AI-based deepfake technology, the scammers replicate facial features, expressions, and even voices of other individuals in real-time to establish trust and elicit financial transactions from unsuspecting victims. According to the FBI, romance scams have resulted in financial losses exceeding over $650 million, emphasising the growing sophistication of cybercriminal tactics.

- **Potential Targets**: individuals using online social platforms.
- **Mitigation Strategy**: identity verification measures for online social platforms and teleconference. Raise awareness about suspicious money or information requests. Strengthen social media privacy settings, use secure communication, and stay updated on deepfake tech. Report suspicious activities to authorities or platforms to prevent further issues.
- **Criticality: High** - real-time face-swapping deepfake technology represents a notable security risk.

Costa Rica Advances into the Digital Era with New Digital ID Initiative

By the end of 2025, Costa Ricans will have the option to store a digital ID in a smartphone app instead of carrying a physical card. Users will need to register through the Supreme Electoral Tribunal, ensure that their biometrics are current, and have a physical ID. This initiative, mirroring moves in the EU and beyond, aims to secure and streamline online transactions with biometric verification, reflecting Costa Rica's commitment to digital transformation and enhanced security.

Australia Advances Digital ID Infrastructure with Comprehensive National and Regional Initiatives

Australia is developing its digital transformation journey with significant investments in its national digital identity program, including AU$288.1 million earmarked for the initiative that began in July 2024. This investment aims to modernise the myGovID platform, enhance security, and engage in pilot programs with the private sector. Concurrently, the Northern Territory has allocated AU$20.6 million for digital driver licenses, adding to the growing list of Australian regions adopting mobile ID solutions. These efforts align with global trends of digital identity systems, underscored by public consultations and robust data protection measures to combat identity fraud. Additionally, the government introduced the Digital ID Bill 2024 and the Digital ID (Transitional and Consequential Provisions) Bill 2023 to Parliament.

New Zealand's Push for Enhanced Biometric Protections and Digital Identity Advancements

The Office of the Privacy Commissioner of New Zealand is seeking public feedback on draft rules concerning the use of biometrics, aiming for refined guidelines that ensure special protections for this data. New Zealand is actively shaping its digital identity landscape through comprehensive reviews and updates to the Digital Identity Trust Framework (DISTF) Act, marked by extensive stakeholder engagement and consultations. Parallel to this, debates around biometric regulations and the Consumer Data Right (CDR)/Credit Reporting Privacy (CRP) bill signify a move towards more stringent controls in specific digital ID applications.

Global Data Safety Issue: Multi-Platform Breaches Compromise Millions

Modality: **Data Breach, Identity Theft, Biometric Information Theft** Attack Instrument: **Unauthorised access, hacking, data infiltration** Location: **Global** Date of report: **May 2024**

In a significant series of data breaches, millions globally have had their personal information compromised.

In Australia, where about one million people had their face biometrics, driver licenses, and even gambling records leaked. An IT provider called Outabox, embroiled in a wages dispute with its former developers, was the target.

Meanwhile, Dell Technologies revealed a breach that has exposed 49 million customers' names, addresses, and purchase details. Although financial data remains safe, the leak puts countless people at risk of phishing and identity theft. A threat actor was involved trying to sell these records online.

Additionally, global ticketing giant Ticketmaster fell victim to the notorious hacker group 'ShinyHunters.' They group siphoned off 1.3 terabytes of data, impacting 560 million users. Names, addresses, credit card details, and more was leaked; the stolen data is now making rounds on the dark web, offered for $750,000 AUD.

- **Potential Targets:** patrons using dining and hospitality apps; tech-savvy consumers and professionals, encompassing both individual and corporate Dell users who rely on technology and enterprise solutions; and global event enthusiasts purchasing tickets for concerts, sports, theater, and other entertainment through high-traffic ticketing services such as Ticketmaster.
- **Mitigation Strategy:** various strategies are recommended to safeguard the integrity of these targets. Implement independent biometric testing, enhance data encryption, improve contract management, secure biometric data storage, and increase security training for stakeholders. Engage in a third-party forensic investigation, strengthen cyber defences, and heighten customer alert protocols against suspicious activity. Establish robust cybersecurity frameworks, transparent incident communication, immediate notification protocols, and enhanced data protection measures, including encryption and multi-factor authentication. Customers should monitor and secure personal information vigilantly.
- **Criticality: High** - the risks encompass identity theft, financial fraud, social engineering attacks, and broader implications for all affected individuals and businesses.

Extensive Data Breaches Unveil Systemic Vulnerabilities in El Salvador and Bangladesh

Modality: **Biometric Data Breach** Attack Instrument: **Illegal Access/Distribution** Location:**El Salvador and Bangladesh** Date of report: **June 2024**

Recent data breaches in El Salvador and Bangladesh have revealed critical weaknesses in handling sensitive data. In El Salvador, 5.1 million citizens' personal and biometric data were exposed by the threat actor 'CiberinteligenciaSV.' The leaked 144 GB data set includes high-definition photos with national ID document numbers, names, birth dates, and more. Meanwhile, in Bangladesh, two high-ranking police officers are accused of accessing and selling citizens' data, including national identity details and phone call records, on Telegram. These breaches highlight systemic vulnerabilities and raise significant concerns about data security and governance.

- **Potential Targets**: citizens face risks of identity theft, financial fraud, and misuse of biometric data. Government officials are vulnerable to exploitation and misuse of sensitive information.
- **Mitigation Strategy**: encrypt and isolate biometric data from personal data, invest in technologies like Presentation Attack Detection, enhance internal monitoring and audit trails for data access, educate citizens on digital hygiene and identity protection, implement stricter controls within government agencies.
- **Criticality: High** - these breaches expose significant vulnerabilities, highlighting the urgent need for enhanced security measures, stricter data governance, and robust regulatory frameworks to protect sensitive information and maintain public trust.

Critical Vulnerabilities in ZKTeco Biometric Terminals Affecting High-Security Environments

Modality: **Biometric Authentication** Attack Instrument: **Code** Location: **Global** Date of report: **June 2024**

Kaspersky researchers uncovered 24 critical vulnerabilities in ZKTeco biometric terminals, extensively used in high-security environments including nuclear power plants, chemical plants, and hospitals. These vulnerabilities can enable threat actors to bypass authentication, steal sensitive biometric data, and gain full control over the terminals. The specific flaws identified include six SQL injection, seven buffer stack overflow, five command injection, four arbitrary file write, and two arbitrary file read vulnerabilities. Key vulnerabilities allow physical bypass using fake QR codes, biometric data theft, and remote code execution.

- **Potential Targets:** high-security installations like nuclear power plants, chemical plants, hospitals, executive suites, and server rooms. Any facility deploying ZKTeco biometric terminals, which may be white-labelled under various brands, is at risk.
- **Mitigation Strategy:** isolating biometric readers on a separate network segment, employing robust administrator passwords, auditing security settings, minimising QR code functionality, and regularly updating firmware. Enhancing biometric terminal security is critically important, given the potential severe consequences of unauthorised access and data breaches.
- **Criticality: Medium** - the potential for unauthorised access to secure areas, data theft, and sophisticated cyber-attacks, compounded by the sensitivity and volume of stored biometric data, marks this issue as a significant cyber threat. Immediate patching and comprehensive security audits are essential to protect against exploitation. protect against exploitation.

Nigeria's NIMC Responds to Data Breach Accusations and Identifies Data Harvesting Websites

Modality: **Digital Data Management** Attack Instrument: **Unauthorised data collection, phishing, fake webs** Location: **Nigeria** Date of report: **June 2024**

The National Identity Management Commission of Nigeria (NIMC) is working to dispel accusations of data breaches related to its biometric national digital ID database. Reacting to concerns raised by Paradigm Initiative, a digital rights group, NIMC's Head of Corporate Communications, Kayode Adegoke, assured that the national identity registry remains secure. He flagged five websites illegally collecting personal data under the guise of issuing National Identification Numbers (NIN). The World Bank made enacting the Data Protection Law a condition of its $430 million grant to NIMC to support NIN issuance, and has disbursed $45.5 million of the total so far, Nairametrics reports.

- **Potential Targets:** Nigerian citizens, particularly those seeking to obtain or manage their National Identification Numbers (NIN). Unauthorised data gathering could significantly compromise the security and privacy of sensitive biometric data.
- **Mitigation Strategy:** NIMC advises citizens to refrain from using unverified websites for personal data submission, underscores its compliance with ISO 27001:2013 standards and the Nigerian Data Protection Law, affirming its commitment to secure data management practices.
- **Criticality:** Medium - risks to individuals' privacy leading to widespread identity theft and fraudulent activities. Immediate action and continuous vigilance are essential to protect data integrity and trust in national identity infrastructure.

White Hat Hacker Exposes Vulnerability in Germany's Digital ID

Modality: **Digital Communication, Identity Authentication** Attack Instrument: **Man-in-the-Middle (MitM) Attack** Location: **Germany** Date of report: **February 2024**

A white hat hacker named CtrlAlt discovered a major vulnerability in Germany's digital ID system (eID), risking Man-in-the-Middle attacks for about 10 million users. By manipulating the official eID app's open-source code, the hacker showed how an application could log the six-digit PIN entered on smartphones. This could let malicious actors intercept data and access key services like government, eHealth, and banking systems. Despite the hacker reporting this to Germany's Federal Office for Information Security (BSI), the BSI downplayed the immediate risk.

- **Potential Targets:** German citizens using digital ID services including government platforms, eHealth applications, and online banking systems. Individuals using smartphones for digital ID authentication are particularly at risk from malware.
- **Mitigation Strategy:** enhance user awareness through cybersecurity training, implement stronger malware detection and prevention protocols, and introduce multi-factor authentication for the eID system. Regular reviews and security updates for the eID app and associated devices are also crucial.
- **Criticality:** Medium - the exposure of German eID vulnerabilities highlights a critical security threat, given the extensive reliance on digital IDs for various secure services and the potential for significant data breaches and identity theft. Strengthening digital ID security and user device protection remains imperative.

Summary

The second quarter of 2024 has seen a significant increase in identity-related vulnerabilities, with numerous threats ranging from sophisticated biometric data breaches to the rising exploitation of deepfake technologies in social engineering attacks. Key incidents such as the compromise of biometric systems in high-security environments and large-scale data leaks in countries like Bangladesh and El Salvador underscore the critical importance of securing both personal and biometric data. The development of digital identity systems globally, including in Australia, Belgium, and Costa Rica, further highlights the need for robust privacy safeguards and ongoing innovation to counter evolving threats. As digital transformation accelerates across sectors, governments and organisations are increasingly targeted by cybercriminals, necessitating proactive measures to protect citizens and infrastructure from identity fraud, phishing attacks, and unauthorised data collection.

Next Steps

1. **Strengthening Biometric and Identity Verification Systems**: Implementing advanced encryption, multi-factor authentication, and regular security audits for identity and biometric data systems is essential to safeguard against unauthorised access and misuse.
2. **Educating Users on Digital Security**: Raising public awareness around the risks of deepfake technologies, phishing, and identity theft can significantly reduce the risk of individuals falling victim to these evolving scams.
3. **Enhancing Collaboration with Security Experts**: Engage with cybersecurity professionals to monitor new threats and update security protocols. Regular engagement with third-party specialists for security audits and vulnerability assessments is crucial for staying ahead of attackers.
4. **Maintaining Vigilance in Data Protection**: With new digital identity frameworks rolling out globally, it is critical to ensure that data governance frameworks are aligned with international standards such as GDPR, ensuring strong protections for both personal and biometric data.

By addressing these vulnerabilities head-on and strengthening digital identity systems, organisations can help reduce risks, maintain public trust, and protect the integrity of their services in an increasingly digital world. For further information or assistance with implementing these recommendations, contact BixeLab at info@bixelab.com or visit our website.