



Training Unit 2: Digital Security in Tourism

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

TABLE OF CONTENTS

INTRODUCTION.....	3
TRAINING UNIT 2: DIGITAL SECURITY IN TOURISM	4
Course objectives.....	4
Learning outcomes.....	4
Unit's framework and methodology	5
2.1 Fundamentals of Digital Security	7
1. Why Digital Security is Critical in Tourism.....	7
2. Core Cybersecurity Concepts	10
3. Cyber Hygiene in Tourism Workplaces	13
4. Human Factor, Social Engineering and Disinformation	16
5. Regulatory Basics: GDPR and NIS2 in Tourism.....	20
6. Roles, Responsibilities and Escalation	23
7. Digital Security in Everyday Tourism Operations.....	26
8. Knowledge Check & Exercises	30
2.2 Security in Digital Tourism Processes	38
1. Digital Tourism Processes & Risk Points.....	38
2. Secure Customer Data Management.....	43
3. Payment, Fraud and Booking Scams	46
4. Scenario Exercise: Suspicious Payment.....	50
5. First 24 Hours After a Data Breach.....	52
6. Cooperation with IT and External Providers.....	56
7. Advanced Technologies in Digital Tourism Security.....	58
8. Reflection & Consolidation.....	62
2.3 Simulations and Digital Crisis Management	65
1. Types of Digital Incidents in Tourism	65
2. Psychological Pressure in Digital Crises	67
3. Case Study 1 – Ransomware Attack on a Hotel Property Management System (PMS)	68
4. Case Study 2 – Booking platform phishing campaign.....	71

Training Unit 2: Digital Security in Tourism

5. Crisis Communication	73
6. Post-Incident Recovery & Trust	76
7. Final Discussion & Evaluation.....	78
REFERENCES	84

LIST OF FIGURES

Figure 1: Tourism data flow and vulnerabilities across OTA, CRS, PMS and payment systems.....	9
Figure 2: Social Engineering Attack Chain.....	17
Figure 3: Key response phases during the first 24 hours after a data breach	53

1

INTRODUCTION

The TREADS project responds to the accelerating digital transformation of the European tourism sector, with particular attention to micro-SMEs and SMEs that form the backbone of the industry. While digitalisation enhances competitiveness and operational efficiency, it also introduces significant risks related to data management, cybersecurity, and disinformation. The tourism sector ranks among the most targeted industries in cyberattacks, highlighting the urgent need for structured education and training that strengthen digital resilience.

At the same time, the EU Pact for Skills for Tourism identifies a persistent skills gap within the sector, especially among small-scale operators, where digital and cybersecurity competences remain unevenly developed. Addressing this gap is essential to ensure a secure and sustainable transition into the digital era.

Within this framework, the present Training Unit 2: *Digital Security in Tourism* deliverable constitutes the structured training curriculum for Training Unit 2: *Digital Security in Tourism* and is designed for implementation as a 48-hour Vocational Education and Training (VET) course. The course focuses on digital security in tourism, covering digital tourism processes and digital crisis management through a combination of theoretical foundations, regulatory awareness, applied exercises, and simulation-based learning. It is aligned with relevant EU policy frameworks and aims to equip VET trainers and learners with practical competences that enhance organisational resilience, responsible digital practices, and structured crisis response in the tourism ecosystem.

Course objectives

This training unit aims to strengthen the capacity of tourism professionals to operate securely within digitally interconnected environments. It provides structured knowledge, applied operational skills, and governance-oriented awareness necessary to manage digital risks in tourism processes.

The unit seeks to:

- Build awareness of systemic digital risks within interconnected tourism ecosystems;
- Reinforce secure operational practices in managing customer data, payments, and reservation systems;
- Align professional behaviour with organisational security policies and EU regulatory requirements;
- Strengthen structured escalation procedures and coordinated incident response;
- Foster digital resilience and sustain customer trust in tourism organisations.

The broader objective of this unit is to support the development of digitally competent tourism professionals who combine technical awareness with responsible behaviour and structured incident response.

Learning outcomes

KNOWLEDGE

By the end of the training, the learner will be able to describe basic digital security concepts and understand the most common digital threats affecting the tourism sector. They will recognize typical vulnerabilities in digital tourism processes, such as online reservation systems, digital payments, and data management practices. The learner will also understand fundamental principles of digital security, including the concept of Zero Trust Security, and will be able to identify basic regulatory requirements related to data protection and digital security, such as the General Data Protection Regulation (GDPR). In addition, they will understand how digital incidents can affect business continuity and the reputation of tourism organizations.

SKILLS

The learner will be able to apply basic digital security practices in daily tourism operations and follow secure procedures when handling customer data, online bookings, and digital payment systems. They will be capable of detecting and reporting suspicious digital activities, such as phishing attempts or online fraud, and of responding appropriately to simulated cyber incidents, including data breaches or ransomware attacks. Furthermore, learners will be able to contribute to internal communication and response procedures during digital crises.

COMPETENCIES

The learner will work responsibly with digital systems and customer data in accordance with established security policies. They will support organizational responses to digital security incidents within their level of responsibility and will be able to adapt their behavior and procedures in order to reduce digital risks in tourism environments.

Unit's framework and methodology

DURATION

48 hours (16 for each subunit)

METHODS OF DELIVERY

The unit can be delivered online, through individual or group-based learning, or in person.

PRACTICAL ACTIVITIES AND RELATED OUTPUTS

Training Unit 2: Digital Security in Tourism

- Basic security assessment of a tourism-related website identifying potential vulnerabilities related to data protection, online bookings, and user access. A short security audit report outlining identified risks and recommended mitigation measures will be prepared afterwards
- Case study on a ransomware attack on a hotel Property Management System (PMS). Learners will analyze a realistic case study focusing on causes, impacts and response actions and will write a case analysis describing the incident, the response strategy and the lessons learned
- Workshop on communication planning for data leak crises: through group work, learners design and draft a communication plan addressing internal and external communication during a data leak or digital security incident and present their work to the trainer and to the other students
- Simulated phishing attacks and online reservation fraud scenarios, followed by a checklist documenting correct responses and improvement areas
- Development of a comprehensive digital security plan for a tourism agency or hotel, including preventive measures, response procedures and roles

The practical activities may be carried out individually or in groups, depending on the context.

ASSESSMENT

- Short quizzes on theoretical knowledge
- Evaluation of the practical activities through, for example, questionnaires, quizzes, hackatons, reports, checklists, group presentations

The learner's achievement will be assessed through their ability to correctly identify digital security risks in practical, tourism-related scenarios. They will be expected to demonstrate the secure use of digital tools during simulations or hands-on exercises, as well as successfully complete phishing or fraud detection simulations.

Assessment will also consider the learner's contribution to the development of a basic digital incident response or communication plan. Finally, learners must pass final assessments that combine theoretical knowledge with practical application.

2.1 Fundamentals of Digital Security

At the end of the sub-unit, learners will be able to recognize unsafe digital behaviour, apply basic security rules in daily work, report incidents correctly, and understand roles and responsibilities.

- Basic concepts of digital security
 - Cyber hygiene (password management, MFA, updates, backups)
 - Human factor in digital security
 - Regulatory framework (GDPR basics for tourism staff), NIS2 Directive (overview, relevance for tourism supply chain)
- Most common digital threats in the tourism sector
- Disinformation and social engineering targeting tourism businesses (fake reviews, false alerts, manipulated customer communications)
- Introduction to Zero Trust Security

Suggested practical activity:

- Digital security awareness quiz

1. Why Digital Security is Critical in Tourism

Digital security plays a critical role in the tourism sector, where organizations continuously collect and process personal and payment data across interconnected digital environments. Booking systems, online platforms, and payment services exchange data in real time to enable reservations, check-ins, and financial transactions. High transaction volumes, extensive reliance on external partners, and permanent system accessibility significantly expand the attack surface, increasing exposure to operational errors, misuse, and cyberattacks. Because these systems are tightly connected, even a small weakness in one part of the digital chain can have wide-ranging consequences for guests, staff, and business operations.

Key systems involved in this data flow include:

Training Unit 2: Digital Security in Tourism

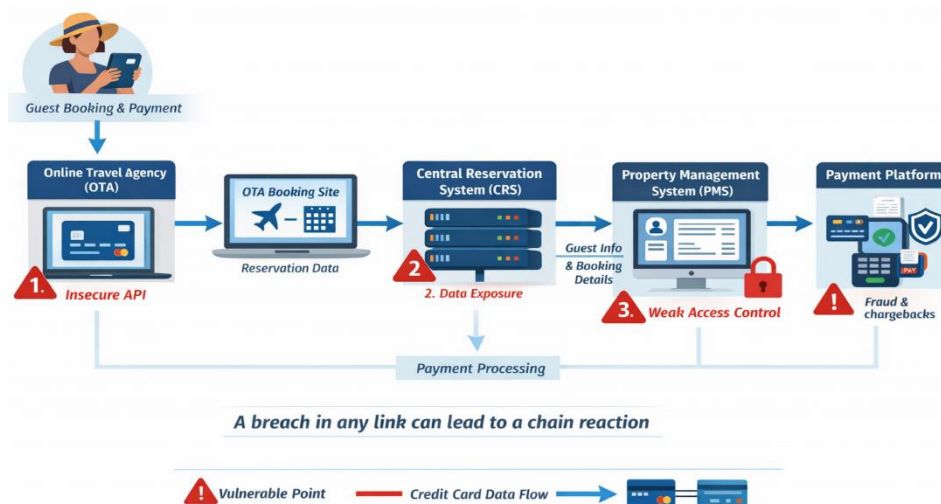
- **Property Management Systems (PMS)** – internal hotel systems used for bookings, check-in, guest records, and billing;
- **Central Reservation Systems (CRS)** – systems that synchronise room availability and prices across multiple booking channels;
- **Payment platforms** – tools that process card payments, refunds, and chargebacks.

Because these systems are interconnected, a weakness in one can affect the others. A typical incident follows a predictable chain:



For example, in real incidents, hotels that continued accepting payments without **3-D Secure** (an additional verification step for cardholders) during major system outages later faced increased chargebacks and financial losses. That risk is why EU rules on trustworthy data sharing and accountability — notably the Data Governance Act¹ — promote mechanisms to "facilitate data sharing across sectors" while increasing trust in data-handling.

Tourism Data Flow and Vulnerabilities



¹ European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868>

Figure 1: Tourism data flow and vulnerabilities across OTA, CRS, PMS and payment systems

The tourism sector is especially exposed because data is constantly shared between partners. A single exposed **API**—a digital interface that allows different software systems to communicate—at an **Online Travel Agency (OTA)** can enable attackers to access large volumes of booking data. Once attackers gain a foothold, they may move through linked systems and cause cascading failures that affect multiple organisations. The ethical dimension of protecting travellers and their data is also explicitly called out in the **UNWTO Global Code of Ethics for Tourism**², which asks that "the public and private stakeholders in tourism development should cooperate in the implementation of these principles" (implementation / cooperation responsibilities).

These incidents result in real-world harm. Guests may face fraud or identity misuse, staff must spend time managing incidents instead of serving customers, and organisations suffer financial and reputational damage. The ethical responsibility to protect guests is also emphasised in the **UNWTO Global Code of Ethics for Tourism**, which states that tourism stakeholders should ensure the protection of tourists and their personal data.

Going Beyond

Digital security risks vary by business model:

- **Hotels** focus on protecting concentrated guest profiles and maintaining uninterrupted daily operations. Incidents often have an immediate operational impact, affecting check-in, billing, and guest experience.
- **Destination Marketing Organizations (DMOs)** rely on shared datasets and partner feeds, which makes them vulnerable to corrupted, delayed, or misleading information that can affect destination reputation and decision-making.
- **Online Travel Agencies (OTAs)** centralize bookings for thousands of suppliers and integrate many partners through technical interfaces. They are particularly exposed to API-related systemic risk, where a single weakness can propagate across multiple organizations simultaneously.

² World Tourism Organization (UNWTO). (n.d.). *Global code of ethics for tourism*.
<https://www.untourism.int/global-code-of-ethics-for-tourism>

Training Unit 2: Digital Security in Tourism

Addressing these risks requires workforce development and digital skills: the tourism skills partnership under the EU Pact for Skills aims to promote upskilling and reskilling of 60% of the workforce each year by 2030 across the ecosystem³, which directly supports improved cyber-awareness and operational resilience.

Reflection & Discussion

01

Why is tourism considered a high-risk sector for digital security?

02

Name two impacts of a digital incident and explain one.

03

Going Beyond: Which business model is most exposed to risks from insecure APIs, and why?

2. Core Cybersecurity Concepts

Digital security risk follows a simple and repeatable logic that applies across most organizations and systems. In most cases, attackers begin by identifying common and easily exploitable weaknesses rather than using highly sophisticated techniques. Typical examples include weak or reused passwords, incorrect system settings, and missing software updates.

When one of these vulnerabilities is exploited, the impact rarely remains limited to a single system. Consequences can quickly include the loss of personal or business data, disruption of services, financial fraud, and additional recovery costs related to investigation, remediation, and lost productivity. Understanding this cause-and-effect logic is essential for recognizing how small weaknesses can escalate into significant operational and business problems.

In tourism environments, risks generally fall into two **interacting categories**:

- **Technical risks**, such as insecure system interfaces (APIs), outdated servers, poorly configured services, and missing security patches.

³ European Commission. (2024). *The EU Pact for Skills – Skills Partnership for the Tourism Ecosystem (Baseline Update)*. European Commission.
https://pact-for-skills.ec.europa.eu/document/download/83968c43-1706-4fbd-9fd0-4461583607d7_en?filename=Pact%20for%20Skills%20Tourism%20Baseline%20-%20update%2020240229.pdf

- **Human-driven risks**, such as phishing, credential misuse, or accidental exposure of personal data.

These risks reinforce each other. For example, a single phishing email can trick a staff member into revealing credentials, which then allows an attacker to exploit an existing technical weakness. Likewise, a technical failure can create confusion or urgency that attackers use to manipulate human behaviour.

Zero Trust as a Practical Security Principle

To reduce the spread of incidents, a widely used security principle is **Zero Trust**. Instead of assuming that users or systems are trustworthy by default, access is granted only after verification. Core elements of this approach include verifying identity, limiting access to what is strictly necessary, separating systems where possible, and monitoring activity for anomalies.

In practice, Zero Trust helps ensure that a compromise of one account or system does not automatically lead to broad access across connected environments. This is particularly important in tourism, where systems are tightly integrated and staff roles change frequently.

Practical Mitigations

At this level, effective mitigations are straightforward and actionable:

- apply regular software updates and security patches to close known vulnerabilities before they can be exploited;
- use strong authentication methods and least-privilege access so that users can access only the systems and data necessary for their role;
- log and monitor suspicious behaviour by keeping records of important system actions and checking them for unusual activity;
- train staff to recognise phishing and other social-engineering techniques so that suspicious messages or requests are identified and reported early.

Together, these measures reduce both technical and human-driven risks and help limit damage when an incident does occur.

Scenario: Verification Under Pressure

A well-known celebrity is staying at your destination. A caller contacts the hotel's front desk, claiming to be the guest's "personal assistant," and requests the room number and a copy of the check-in folio for "tax purposes."

This situation raises important questions:

- **The dilemma:** Does applying Zero Trust mean being suspicious of everyone, even at the risk of offending a VIP?
- **The cooperation challenge:** How can staff verify the caller's identity through proper channels without appearing rude or undermining the hospitality experience?

This scenario highlights how security principles must be applied in a way that respects both protection requirements and the tourism service culture.

Going Beyond

Zero Trust is conceptually effective, but older or legacy systems often lack built-in identity management or access segmentation capabilities. In such environments, organisations rely on **compensating controls**, such as gateway authentication, network segmentation, and enhanced logging, to reduce exposure. Planning staged upgrades alongside interim safeguards is essential to manage risk effectively whilst avoiding disruption to daily operations.

Zero Trust should be understood as a long-term security approach rather than a single technology or quick fix.

Reflection & Discussion

01

What is the difference between a threat and a vulnerability?

02

Give two examples of human-driven risks and describe one simple mitigation.

03

Going Beyond: What is a primary limit when applying Zero Trust to legacy systems?

3. Cyber Hygiene in Tourism Workplaces

Most digital incidents do not start with hackers breaking in, but with ordinary working routines. Routine everyday behaviour strongly influences whether small issues remain minor or develop into major digital incidents.

Typical everyday lapses include:

- using weak or reused passwords (for example, 123456, password);
- postponing or ignoring software updates;
- leaving sessions unlocked on shared devices at the reception or back office;
- saving passwords in browsers on communal computers;
- using unsecured public Wi-Fi for work-related tasks.

In tourism organizations, where personal and payment data are handled daily, these seemingly small lapses can quickly result in exposed data, fraudulent transactions, or service interruptions.

Practical, High-Impact Measures

Practical, high-impact measures focus on reducing everyday digital risks. They are most effective when they are easy to apply and consistently followed. Rather than relying on advanced technology, these measures focus on prevention and the early limitation of damage by strengthening everyday behaviour, access controls, and basic system hygiene.

Key measures include:

- **Using strong and unique passwords** for each system (e.g. BlueCoffee-Flying-Moon!77) and storing them securely in a password manager where available. Passwords should be changed immediately if compromise is suspected, following a security incident, when credentials may have been exposed, or when organisational policy requires it. Routine password changes without evidence of compromise are generally not recommended, as they may encourage weaker password practices and password reuse.
- **Enabling multi-factor authentication (MFA)** to add an additional layer of protection and prevent account takeover even if passwords are stolen;

- **Applying regular software updates and security patches** to close known vulnerabilities before they can be exploited.

Managing Risks on Shared Devices and Remote Work

Shared devices present a specific risk in tourism workplaces, where multiple staff members use the same systems across shifts. Because actions from different users are mixed together, it becomes harder to trace responsibility and easier for unauthorised access to go unnoticed.

Simple and effective mitigations include:

- locking screens when stepping away from a workstation;
- using individual user accounts for each staff member;
- avoiding the storage of passwords in browsers on communal machines.

Secure remote work requires additional care. Staff should use trusted networks or a VPN and avoid public Wi-Fi when performing sensitive work tasks.

Mobile Device Security in Tourism

Mobile devices have become part of everyday work in the tourism sector. Staff often use smartphones and tablets to access email, booking platforms, payment systems, customer information, and communication tools.

If a device is lost, stolen, or compromised, unauthorised individuals may gain access to business systems or sensitive customer data. For this reason, **mobile devices should be protected in the same way as computers and other workplace systems.**

Good practices include:

- using a screen lock (PIN, password, fingerprint, or facial recognition);
- enabling multi-factor authentication (MFA) where available;
- keeping devices and applications with the latest security patches and software updates;
- downloading apps only from trusted sources;

- reporting lost or stolen devices as soon as possible;
- avoiding access to sensitive information through unsecured public Wi-Fi networks.

Simple precautions can significantly reduce the risk of unauthorised access and help protect both organisational and customer information.

Building Secure Habits Through Training

Training plays a critical role in turning security measures into consistent habits. Staff should understand how phishing and social-engineering attacks exploit routine behaviour, such as clicking links or entering credentials under pressure.

Effective training focuses on:

- recognizing suspicious messages and requests;
- knowing when and how to report potential incidents;
- practising escalation steps so that issues are addressed quickly.

Together, these practical controls significantly reduce the likelihood that a single mistake—such as clicking a malicious link or leaving a session unlocked—escalates into a serious incident that harms guests or overloads staff.

Emerging Authentication Methods: Passkeys

Passkeys are an emerging authentication method designed to replace traditional passwords. Instead of relying on memorised credentials, passkeys use cryptographic keys stored securely on a trusted device and are typically unlocked through biometrics (such as fingerprint or facial recognition) or a device PIN.

Key benefits include:

- resistance to phishing attacks;
- elimination of password reuse;
- improved user experience;
- stronger protection against account takeover.

Training Unit 2: Digital Security in Tourism

Major technology providers such as Apple, Google, and Microsoft increasingly support passkeys across consumer and business services. As adoption continues to grow, tourism organisations may encounter passkey-based authentication in reservation systems, cloud platforms, and customer-facing applications.

Going Beyond

Policy design must balance security with practicality. Overly strict and cumbersome rules—such as constant forced password rotation or excessively heavy authentication for basic tasks—can reduce staff compliance. Conversely, overly relaxed controls increase risk exposure. The most effective approach uses targeted controls, clear exceptions, and straightforward procedures, enabling staff to adopt protective habits consistently as part of their daily work.

Reflection & Discussion

01

Which three routine actions most reduce the risk of account takeover, and why?

02

Give one risk associated with shared devices and one simple mitigation.

03

Going Beyond: Why must a cyber hygiene policy balance security and practicality?

4. Human Factor, Social Engineering and Disinformation

Human-focused attacks exploit **trust and routine behaviour**, rather than technical weaknesses. Phishing emails, impersonation calls, and fake supplier requests rely on believable messages to trick staff into sharing credentials, approving payments, or disclosing sensitive information. In tourism environments, attackers often pose as known partners, platforms, or colleagues to create urgency and bypass normal verification steps.

The logic of these attacks is simple and repeatable:



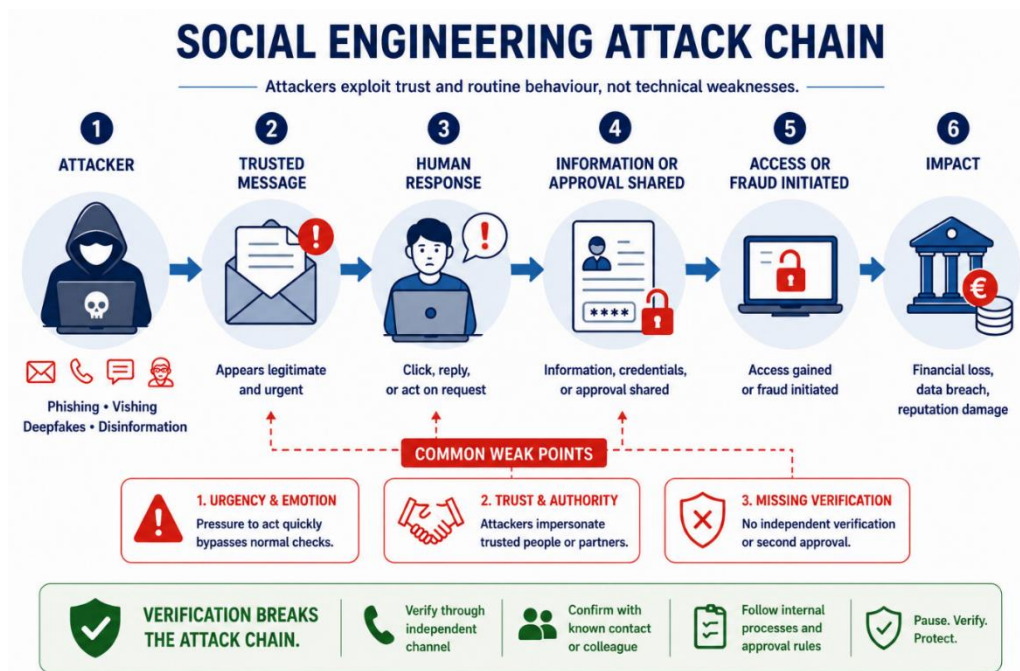


Figure 2: Social Engineering Attack Chain

Practical Scenario: Urgent Supplier Request

A hotel accountant receives an email that appears to come from a long-standing supplier, requesting an urgent change to bank account details. The message uses familiar language and includes a realistic invoice. Because the request is marked as urgent and the sender appears trusted, the accountant feels pressure to act quickly to avoid payment delays.

Use the checklist below to assess the situation:

- ✓ Is the request urgent or emotionally framed?
- ✓ Does it involve money, access, or sensitive data?
- ✓ Does the sender appear familiar and trusted?
- ✓ Can the request be verified through an existing, known contact channel?
- ✓ Is there a requirement for a second approval or internal confirmation?
- ✓ Does the request bypass usual approval or review steps?
- ✓ Are there small inconsistencies (names, signatures, invoice numbers, formatting)?
- ✓ Does the message create pressure to act immediately without giving time to verify?
- ✓ If this request is fraudulent, what would be the potential impact on money, data, or reputation?

Disinformation and Social Engineering in Tourism

Disinformation adds an additional layer of risk to social-engineering attacks. Fake alerts, manipulated online reviews, or spoofed customer messages can mislead both staff and guests, trigger unnecessary actions, and undermine trust in systems and organisations.

Common warning signs of social-engineering attempts include:

- urgent or emotionally charged language;
- unexpected requests involving payments or access;
- mismatched or unusual sender addresses;
- small spelling, formatting, or tone inconsistencies.

The most reliable defensive action is **verification**. Suspicious requests should be confirmed through an independent channel, such as calling a known contact number or checking internally. For financial or sensitive actions, requiring a second approver significantly reduces risk.

Breaking the Attack Chain

Well-designed processes can interrupt social-engineering attacks early. Requiring verification before action, separating duties (for example, different people initiating and approving transactions), and defining clear escalation routes dramatically reduce potential harm. These controls are effective even without changes to core technical systems.

A culture of cautious verification, combined with simple transaction controls, makes it far more difficult for attackers to convert an initial contact into fraud or data loss.

Real-World Example: Reported Ransomware Incident Affecting a European Hotel Chain⁴

In **October 2023**, the European hotel group **Motel One** disclosed that it had been affected by a ransomware attack attributed to the **ALPHV/BlackCat** cybercriminal group. According to public reporting, the incident involved **unauthorised access to**

⁴ Security Week (October 2023). *Motel One Discloses Ransomware Attack Impacting Customer Data*. <https://www.securityweek.com/motel-one-discloses-ransomware-attack-impacting-customer-data/>

customer-related data, including booking information and contact details (SecurityWeek, 2023).

While the company stated that hotel operations continued to function, the attack raised concerns regarding potential exposure of personal data and triggered regulatory and reputational implications. As commonly observed in ransomware incidents, threat actors published claims online regarding the volume of allegedly stolen data; however, such claims may exceed officially confirmed information and should be interpreted cautiously during ongoing investigations.

The case illustrates how weaknesses in administrative access controls and network security can enable large-scale data exposure in the hospitality sector. Even where core services remain operational, ransomware incidents may generate operational disruption, financial impact, regulatory scrutiny, and long-term reputational damage.

This example reinforces the systemic nature of digital risk in tourism ecosystems, where interconnected booking, payment and CRM systems increase the potential impact of cyber incidents across operational, financial and regulatory dimensions.

AI-Enhanced Social Engineering

Social-engineering attacks increasingly make use of artificial intelligence to create more convincing and personalised fraudulent communications. In the past, phishing messages were often easier to identify because they contained spelling mistakes, unusual wording, or other signs that suggested they were not genuine. Today, AI tools can produce professional-looking emails, messages, audio recordings, and even videos that closely resemble legitimate communications.

- AI-generated phishing emails;
- voice-cloning attacks (vishing);
- deepfake video impersonation;
- fake customer messages generated by AI tools;
- prompt-injection attacks targeting AI systems used within organisations;

These techniques make verification more challenging because attackers can imitate trusted individuals or organisations with a high degree of credibility. Managers, suppliers, colleagues, business partners, or customers may all be impersonated in

an attempt to obtain information, gain access to systems, or persuade staff to take actions that they would not normally perform. As a result, organisations should place greater emphasis on verification procedures and independent confirmation of unusual requests, even when communications appear authentic.

Real-World Example: Deepfake Executive Impersonation⁵

In 2024, a multinational engineering company was targeted by attackers who used deepfake technology during a video conference to impersonate senior executives. Believing the meeting to be genuine, an employee authorised a series of transactions that resulted in losses of approximately USD 25 million.

Going Beyond

When analysing the social-engineering attack chain (reconnaissance → contact → exploitation → cashout), the greatest leverage comes from blocking the earliest stages. Strong identity verification, strict transaction approval controls, and mandatory confirmation steps significantly limit attacker movement and reduce downstream impact. These measures remain effective even when full technical upgrades are not yet feasible.

Reflection & Discussion

01

What common tactics do attackers use to trick staff, and what is one direct consequence?

02

Name two warning signs of a scam message and one safe action to take.

03

Going Beyond: Which points in the social-engineering attack chain are most effective to block, and why?

5. Regulatory Basics: GDPR and NIS2 in Tourism

Data protection and digital security in tourism are shaped by two key regulatory frameworks: **GDPR**, which focuses on the protection of personal data and individual rights, and **NIS2**, which focuses on digital service resilience and supply-chain security.

Under **GDPR**, organisations are required to protect personal data through measures such as data minimisation, access controls, and timely breach reporting. **The**

⁵ CNN (2024). Finance worker pays out \$25 million after video call with deepfake “chief financial officer”. <https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>

General Data Protection Regulation (GDPR)⁶ has applied across the European Union since May 2018, establishing a common framework for the protection of personal data and individual privacy. The purpose of GDPR is to safeguard individuals' privacy and to ensure that organisations handling personal data are accountable for how it is collected, stored, and used.

For example, if a scan of a guest's passport is exposed, the organisation must take immediate steps to contain the incident, assess the risk to affected individuals, and, where required, notify the relevant authority and the individuals concerned. Delayed or incomplete action can increase harm to guests and lead to regulatory consequences.

NIS2 and Digital Resilience in the Supply Chain

The NIS2 Directive⁷ is an EU framework that strengthens the security and resilience of digital services and networks. It requires organisations and critical service providers to manage digital risks, ensure service continuity, and report incidents that significantly disrupt operations or affect connected partners.

While GDPR focuses on personal data, **NIS2 addresses the resilience and continuity of digital services**. It places increased expectations on organisations and critical service providers to manage digital risk and to report incidents that disrupt or threaten service availability.

For example, a compromised payment gateway that prevents card processing across multiple hotels demonstrates why resilience and supplier incident reporting are essential. When one provider fails, the impact can spread quickly to connected organisations.

NIS2 strengthens requirements for risk management and incident reporting across critical suppliers and service providers. Because tourism organisations rely heavily on external systems—such as **PMS, CRS, and payment platforms**—weak controls at a vendor level can transmit risk through the entire supply chain. Poor compliance

⁶ European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

⁷ European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

or delayed notifications extend the time needed to contain incidents and increase the likelihood of regulatory escalation, including higher fines, mandatory public disclosures, and wider service disruption affecting partners and customers.

The European Union Agency for Cybersecurity (ENISA, 2025)⁸ provides detailed technical guidance on implementing cybersecurity risk management measures under the NIS2 framework. The guidance emphasises structured risk assessment, incident detection and reporting procedures, supply-chain security controls, and continuous improvement mechanisms — all of which are directly relevant for interconnected tourism ecosystems.

Practical Steps to Reduce Regulatory and Operational Risk

To reduce exposure and improve compliance, organisations should focus on practical, coordinated actions:

- minimising the amount of personal data collected and retained;
- clearly defining roles and responsibilities in contracts with vendors and partners;
- enforcing access controls and encryption where appropriate;
- ensuring staff understand when and how to report incidents;
- testing incident response and communication procedures with key suppliers.

These measures shorten detection and response times, limit legal exposure, and help maintain customer trust during and after incidents.

Going Beyond

Failures in GDPR compliance—such as delayed breach notification, incomplete supplier agreements, or inadequate incident logging—reduce the window for effective containment. When combined with interconnected systems, these failures can allow threats to spread to partners, trigger escalated enforcement action, and transform a local data breach into a multi-organisation crisis affecting the wider tourism ecosystem. This illustrates how compliance failures can amplify both the scale and the impact of digital incidents beyond the 22 organization directly affected.

⁸ European Union Agency for Cybersecurity (ENISA). (2025). *Technical implementation guidance on cybersecurity risk management measures (Version 1.0)*.
https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Reflection & Discussion

01

Explain two GDPR obligations that staff must follow and why they matter.

02

Name three typical systems that increase exposure and describe one way a breach in any of them can affect individuals and business operations.

03

Going Beyond: How can a failure in GDPR compliance escalate an incident across a digital supply chain?

6. Roles, Responsibilities and Escalation

Clear roles and timely escalation are essential when a digital incident occurs. As soon as an issue is detected, it must be reported immediately to the designated contact. This initial step is critical because early reporting preserves evidence and triggers a coordinated response, rather than isolated or improvised actions.

In most organisations, incident response involves several defined roles:

- the **incident reporter**, who notices and reports the issue;
- a **first responder** (often IT or security staff), who confirms that an incident has occurred;
- an **incident manager**, who coordinates decisions and response activities;
- **IT or security teams**, who carry out technical containment and recovery;
- **communications**, who manage internal and external messages to stakeholders;
- **legal or compliance**, who assess regulatory, contractual, and reporting obligations.

Each role focuses on a specific responsibility, ensuring that technical, legal, and reputational risks are addressed in parallel and handled correctly.

International standards such as ISO/IEC 27001:2022⁹ emphasise the importance of clearly defined roles, documented procedures, and structured incident response as part of an Information Security Management System (ISMS). These principles reinforce the need for accountability and controlled escalation within tourism organisations.

The Importance of Documentation

Thorough documentation at every stage of an incident is critical. Recording **what happened, when actions were taken, and who approved decisions** creates a reliable audit trail. This supports investigations, regulatory reporting, and post-incident learning. Good documentation also shortens recovery time by allowing teams to see which actions were effective and to avoid repeating mistakes. Importantly, it protects both staff and the organisation if decisions are later reviewed by management, regulators, or partners.

Why Incidents Should Not Be Fixed Individually

Employees must not attempt to fix digital incidents on their own. Acting independently can destroy forensic evidence, unintentionally expand the scope of a breach, or cause additional data loss. Instead, staff should follow instructions from the incident manager or IT/security team, allowing controlled containment and correct notification steps.

It is important to recognise that digital incidents affect real people and real jobs. Customers may suffer harm, staff workloads increase during incidents, and organisational consequences become more severe when escalation is delayed or mishandled.

Going Beyond

Simple responsibility models, such as a **RACI matrix**, help clarify roles under pressure by defining who does what during an incident. In a RACI model:

- **Responsible** refers to the person or team who carries out the task;

⁹ International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
<https://www.iso.org/standard/27001>

Training Unit 2: Digital Security in Tourism

- **Accountable** is the person who has final responsibility and approves decisions;
- **Consulted** includes those who provide input or expertise;
- **Informed** includes those who are kept up to date on progress.

For incident detection, the staff member who notices and reports the issue is Responsible, while the incident manager is Accountable. For incident containment, IT or security teams are Responsible, and the incident manager remains Accountable, with relevant support teams consulted and key stakeholders informed.

This structured approach reduces confusion, prevents duplicated effort, and speeds up decision-making during limited response windows.

Reflection & Discussion

01

Why should employees avoid trying to resolve digital incidents on their own?

02

Name two reasons why documentation is important during an incident.

03

Going Beyond: In the RACI example above, who is responsible for containment and who is accountable?

Incident response for Small Tourism Businesses

Many tourism businesses are small organisations where the owner, manager, or a few employees perform multiple roles. Dedicated cybersecurity teams are often unavailable, which means that incident response procedures need to be practical and easy to follow.

A simple response model can help organisations react quickly when a cyber incident occurs:

Training Unit 2: Digital Security in Tourism

1. Detect	recognise suspicious activity or unusual behaviour
2. Contain	limit the impact by isolating affected devices, accounts, or systems where possible.
3. Report	inform the appropriate person, external IT support, service provider, or relevant authority.
4. Recover	restore normal operations and identify lessons that can help prevent similar incidents in the future.

Even small organisations can respond effectively if staff know what to do and whom to contact. Simple procedures, timely reporting, and clear responsibilities are often more important than complex technical solutions.

7. Digital Security in Everyday Tourism Operations

Digital security becomes effective **only when it is integrated into everyday operational behaviour**. The concepts introduced throughout this unit - including cyber hygiene, awareness of social engineering risks, secure communication, and responsible handling of customer data - are most important in everyday work situations. Digital incidents rarely begin with sophisticated attacks. More often, they **emerge from small operational shortcuts** taken during busy periods, when **staff are under pressure, focused on speed, or managing multiple requests**. Although these actions may seem insignificant, everyday decisions directly influence digital risk.

The cause-and-effect pattern is simple:



One shortcut may not cause harm. But repeated shortcuts weaken protective barriers. Over time, this creates **structural vulnerabilities** that attackers can exploit.

How Everyday Decisions Increase Risk

Common operational behaviours that increase exposure include:

- Reusing login credentials “just for today”
- Delaying system updates because operations are busy
- Sharing access to speed up processes
- Ignoring minor warning messages
- Postponing incident reporting

Individually, these actions seem minor. Repeated over time, they reduce **accountability, traceability, and system integrity**. This increases the likelihood of **data exposure, fraud, or service disruption**.

Awareness is important: operational efficiency and digital safety must support each other, not compete.

Typical Grey-Zone Situations

Grey zones are situations where staff must choose between speed and strict procedure. They are not intentional violations, but judgement moments.

Example 1 – Shared Login During Busy Period

A staff member keeps a system logged in to avoid repeated authentication.

Risk: unattended access, unauthorised actions, data misuse.

Example 2 – Temporary Credential Sharing

Access is shared to help a colleague start work quickly.

Risk: loss of traceability, compliance breach, inability to investigate incidents.

Example 3 – Delayed Reporting

An unusual system message appears near shift end and is not reported immediately. Risk: delayed containment, escalation of technical damage.

In each case, the immediate goal is convenience. The long-term result may be **increased exposure and reduced control**.

Why Small Deviations Lead to Incidents

When unsafe shortcuts are repeated, they become normal behaviour. Over time, staff may stop recognising the risk.

Example progression:

- “Just this once” password sharing
- Repeated sharing
- Multiple people using one account
- No clear responsibility
- Difficult investigation after a breach

Digital incidents often occur when multiple small weaknesses align at the same time.

This is why:

- Clear roles matter
- Consistent reporting matters
- Cyber hygiene habits matter

Strong digital security is built through daily discipline, not only through technical tools. Digital security reflects the interaction between technical controls and behavioural discipline. When daily routines ignore small rules, the organisation slowly loses control over who can access data, change information, or detect problems early. This reduces **visibility, accountability, and response speed**. As control decreases, the probability of **data breaches, financial loss, legal consequences, and reputational damage** increases. Everyday discipline therefore protects both the organisation and the people who depend on its systems.

Going Beyond

Small operational shortcuts do not only increase technical risk; they reveal weaknesses in **risk culture and control systems**. When grey-zone decisions are

frequent, it may indicate unclear accountability, insufficient supervision, or misaligned performance pressures (e.g., speed rewarded more than security).

Advanced analysis focuses on identifying:

- Where shortcuts most often occur
- Why staff feel pressure to bypass controls

Which barriers failed (technical, procedural, or managerial)

- How multiple minor weaknesses combined into one incident

Instead of asking “Who made the mistake?”, advanced risk management asks: **Which control layer failed, and how can the system be strengthened?**

Improving digital resilience therefore requires both:

- Technical safeguards
- Organisational alignment between efficiency and security expectations

Reflection & Discussion

01

Why can small operational shortcuts increase digital risk over time?

02

What is a grey-zone situation in digital security?

03

Why is it important to analyse control failures instead of focusing only on individual mistakes?

Supplementary Video Resources

A supplementary introductory resource is provided by Simplilearn (2023), offering an overview of cybersecurity concepts and threat types.

Channel: Simplilearn

Year: 2023

Title: What Is Cyber Security | How It Works?

YouTube: <https://www.youtube.com/watch?v=inWWhr5tnEA>

8. Knowledge Check & Exercises

Digital Security Awareness Quiz

Objective: Assess understanding of core cybersecurity concepts, cyber hygiene practices, and regulatory basics.

Format: Individual assessment

Estimated Duration: 20–30 minutes

Questions:

1. Why is tourism considered a high-risk sector for digital security?
 - A. Tourism uses more cloud systems than other industries.
 - B. Tourism relies on high transaction volumes and interconnected digital systems.
 - C. Tourism businesses do not train staff in IT.
 - D. Tourism handles little personal data.

Correct answer: B

2. Which of the following best describes a vulnerability?
 - A. A type of malware.
 - B. A weakness that can be exploited by a threat.
 - C. A regulatory requirement.
 - D. A security incident.

Correct answer: B

3. Which actions reduce the risk of account takeover? (Select TWO answers)
 - A. Enabling multi-factor authentication (MFA).

- B. Sharing passwords during peak season to speed up work.
- C. Using strong and unique passwords.
- D. Leaving sessions open for faster shift transitions.

Correct answer: A, C

4. A staff member receives an urgent email requesting immediate payment detail changes from a known supplier. What is the safest action?
- A. Update the payment details immediately to avoid service disruption.
 - B. Forward the email to colleagues for confirmation.
 - C. Verify the request using an independent channel (e.g., calling a known number).
 - D. Ignore the message.

Correct answer: C

5. Under GDPR, organisations must (Select THREE answers):
- A. Protect personal data through appropriate controls.
 - B. Notify authorities when required in case of a data breach.
 - C. Store all customer data indefinitely.
 - D. Limit data collection to what is necessary.

Correct answer: A, B, D

6. What is the main purpose of the NIS2 Directive?
- A. To eliminate all cyber incidents.
 - B. To strengthen digital service resilience and incident reporting.
 - C. To regulate tourism pricing.
 - D. To increase IT outsourcing.

Correct answer: B

7. Why are shared accounts in tourism workplaces risky?
- A. They improve operational speed.
 - B. They reduce accountability and traceability.
 - C. They make it easier to investigate incidents.
 - D. They simplify compliance reporting.

Correct answer: B

8. Which situation represents a “grey zone” decision?
- A. Locking a computer when leaving the desk.
 - B. Refusing to share login credentials under pressure.
 - C. Leaving a system logged in during peak season to avoid repeated authentication.
 - D. Reporting suspicious activity immediately.

Correct answer: C

9. Why should employees avoid fixing digital incidents alone? (Select TWO answers)
- A. It may destroy evidence or expand the breach.
 - B. It demonstrates initiative.
 - C. It ensures faster resolution.
 - D. It may violate internal escalation procedures.

Correct answer: A, D

10. In a RACI model during incident containment, who is typically Accountable?
- A. The IT technician performing the fix.

- B. The incident manager coordinating the response.
- C. The staff member who reported the issue.
- D. The customer affected by the incident.

Correct answer: B

11. Why do small operational shortcuts accumulate into incidents?

- A. They increase system speed.
- B. They normalise unsafe behaviour over time.
- C. They automatically trigger alerts.
- D. They eliminate the need for reporting.

Correct answer: B

12. Which behaviour best supports digital resilience in tourism?

- A. Ignoring minor warning messages during busy periods.
- B. Reporting unusual activity immediately through defined channels.
- C. Sharing system access with trusted colleagues.
- D. Postponing updates until the end of the season.

Correct answer: B

13. Why must the response to a possible data breach follow defined procedures rather than informal decisions?

- A. To avoid destroying evidence and ensure regulatory compliance.
- B. To reduce workload for management.
- C. Because only external partners are responsible.
- D. Because digital incidents resolve automatically if ignored.

Correct answer: A

Exercise 1 – Phishing Red Flag Identification

Objective: Strengthen the ability to detect phishing and social-engineering attempts in tourism communication environments.

Format: Group discussion or plenary analysis.

Estimated Duration: 20–25 minutes.

Participants analyse a simulated suspicious email and identify indicators of potential fraud.

From: Booking Support <support@booking-example.com>

To: Hotel Front Desk

Subject: URGENT: Update Bank Details for Upcoming Payments

Dear Hotel Team,

Please urgently update the bank account for upcoming guest payments. Attached is the latest invoice.

Failure to update may delay payments.

Thank you,

Booking Support Team

Attachment: Invoice_0723.pdf

Red Flags to consider (discussion):

- 🚩 Urgency / pressure language
- 🚩 Unexpected attachment
- 🚩 Generic greeting (“Hotel Team”)
- 🚩 Sender domain slightly off or unfamiliar

Exercise 2 – Digital Risk Prioritisation Sorting

Objective: Develop structured judgement in evaluating operational digital risks.

Format: Small group activity.

Estimated Duration: 25–30 minutes.

Participants rank listed behaviours according to a) likelihood of occurrence, b) potential impact if exploited and c) escalation priority. Participants must provide a short written justification (2–3 sentences) for their ranking decisions, explaining how likelihood and impact interact and why certain behaviours require higher escalation.

Behaviours to rank by severity or likelihood:

- ❖ Leaving sessions open on shared computers
- ❖ Using weak or repeated passwords
- ❖ Sharing credentials with colleagues
- ❖ Clicking links from unknown senders
- ❖ Ignoring system or software alerts
- ❖ Delaying software updates
- ❖ Connecting personal devices to work systems without approval
- ❖ Forwarding emails with sensitive information

Exercise 3 – Regulatory Framework Application

Objective: Ensure correct understanding of key regulatory frameworks and their operational implications.

Format: Individual exercise.

Estimated Duration: 5-10 minutes.

Match each regulatory framework with its core purpose. Then, provide one practical tourism example where the regulation applies.

Terms	Purposes
GDPR	Protect personal data and ensure privacy compliance
NIS2 Directive	Strengthen digital service resilience and incident reporting
Data Governance Act	Regulate responsible data use and sharing across organizations
UNWTO Global Code of Ethics	Promote ethical practices and sustainable tourism

Exercise 4 – Structured Debate: Speed vs Security

Statement for discussion: “Staff should be allowed to bypass verification steps during peak season to maintain operational speed.”

Objective: Develop critical thinking regarding the trade-off between operational efficiency and digital security.

Format: Structured debate (Pro vs Con teams).

Estimated Duration: 25-30 minutes.

Teams prepare arguments addressing:

- operational efficiency pressures,
- security risk amplification,
- regulatory implications,
- impact on guests, staff, and organisational reputation.

Finish with group reflection on balancing speed vs security.

2.2 Security in Digital Tourism Processes

At the end of this sub-unit, students will be able to follow secure procedures for bookings and payments, handle customer data responsibly, act correctly during a suspected data breach, collaborate with IT and security teams.

- Secure customer data management: protection of online reservations and payments
- Blockchain for payments and beyond payments (traceability, identity verification, loyalty programs)
- Response protocols for data breaches (roles and responsibilities in the first 24 hours)

Suggested practical activity:

- Scenario-based exercise: suspicious payment activity

1. Digital Tourism Processes & Risk Points

Digital tourism processes are embedded in nearly every stage of guest interaction. From the moment a reservation is made until after the stay is completed, customer data moves through multiple systems. These processes are designed for efficiency and service quality, yet each digital interaction introduces potential exposure.

A digital risk point occurs whenever data is created, entered, modified, stored, transmitted, or accessed. The more complex and interconnected a process becomes, the more frequently data transitions between systems and users. Each transition increases exposure to both accidental errors and intentional misuse.

The relationship between process complexity and risk follows a cumulative logic:

- more systems involved → more integration points;
- more users involved → more access credentials;
- more automated exchanges → more configuration dependencies;
- more external partners → more supply-chain exposure.

Where Risk Points Commonly Appear

Risk points in tourism processes most often occur in the following operational situations:

1. **Data Entry and Reservation Handling:** Manual data entry into PMS or CRS systems introduces the possibility of errors, duplication, or accidental disclosure. If authentication controls are weak, unauthorised individuals may gain access to reservation data.
2. **Payment Processing:** Payment stages represent high-value targets because they involve financial data. Risks include:
 - insecure payment connections;
 - unusual transaction patterns;
 - mismatched billing information;
 - repeated failed authorisations;
 - card-not-present fraud.

If anomalies are not recognised or reported, financial loss and chargebacks may follow.

3. **System-to-System Transfers:** Automated integrations between PMS, CRM, booking platforms, and payment gateways improve efficiency but introduce dependency risks. Misconfigurations or compromised credentials in one system can propagate across connected platforms.
4. **Access Management and Shift Changes:** Changes in user permissions, shared terminals, and shift transitions create moments of reduced accountability. Temporary shortcuts may weaken traceability and complicate incident investigation.

Interaction Between Technical and Human Risk

Operational risk points reflect the interaction between technical vulnerabilities and human behaviour. A technical weakness, such as an insecure configuration, may remain dormant until triggered by a human error. Conversely, a minor human shortcut can expose a system vulnerability that would otherwise remain harmless.

For example:

- A receptionist reuses credentials to speed up check-in.
- A compromised email account is used to reset a password.
- A delayed update leaves a known vulnerability unpatched.

Individually, these actions may appear minor. In combination, they can create conditions for significant incidents.

Physical Digital Hygiene

Digital risks in tourism environments are not limited to software and data flows. Many incidents originate from **physical access to digital systems**, particularly in operational settings such as hotel receptions, shared workstations, or back-office areas.

Unattended devices, weak control over physical access, or the use of external devices can create entry points for attackers. In highly dynamic environments with multiple staff shifts and guest interaction, these risks are amplified.

Typical examples include:

- leaving a check-in terminal unattended while logged in;
- allowing access to back-office areas or server rooms without supervision;
- connecting unknown USB devices to operational computers;
- displaying sensitive information on screens visible to guests.

Even simple actions, such as leaving a server room door open for ventilation, can undermine otherwise robust digital security measures.

For this reason, physical digital hygiene should be considered part of everyday operational behaviour, complementing technical controls and reducing the likelihood that minor oversights develop into larger incidents.

Structured Risk Prioritisation in Tourism Operations

Digital risk in tourism environments should not be evaluated intuitively but through structured prioritisation. Two primary dimensions determine urgency:

- Likelihood (probability of occurrence)
- Impact (operational, financial, regulatory, reputational)

A simplified evaluation grid supports proportional response:

Impact / Likelihood	Low	Medium	High
Low Impact	Low	Low	Low
Medium Impact	Low	Medium	Medium
High Impact	Medium	High	Critical

Risks that combine high impact and high likelihood require immediate attention and mitigation. Lower-priority risks should continue to be monitored, but they may not require the same level of resources or urgency.

The Role of Employees in Managing Risk Points

Employees act as both users and safeguards within digital processes. Their behaviour directly influences whether a risk point escalates.

Staff should:

- follow defined procedures when entering or modifying data;
- verify unusual requests before taking action;
- monitor for irregular transaction patterns;
- avoid sharing credentials, even temporarily;
- report suspected irregularities immediately through defined channels.

As emphasised in Sub-unit 2.1, early escalation is critical to prevent localised irregularities from developing into systemic incidents. In operational contexts such as payment processing and booking management, delayed reporting significantly increases financial and regulatory exposure.

Digital incidents in tourism processes have tangible consequences. Guests may experience financial loss or privacy breaches, and organisations may face reputational damage or regulatory obligations. Operational continuity depends on responsible behaviour at every digital step.

Going Beyond

Risk mapping across the full digital customer journey provides a structured method for analysing exposure. Instead of evaluating isolated tasks, organisations examine:

- where data is collected;
- where it is stored;
- where it is transferred between systems;
- where permissions change;
- where external providers are involved.

Risk is typically highest at transition points, particularly where data changes ownership or system control. Mapping these stages allows organisations to prioritise high-impact control measures rather than distributing resources evenly across all process steps.

Practical Activity: Mapping Risk Points in a Real Tourism Process

Objective: Identify systemic digital risk points across a selected tourism process.

Format: Small group workshop (3–4 participants)

Estimated Duration: 45–60 minutes

In small groups, choose one common tourism process, for example:

- handling an online reservation;
- processing a refund;
- managing group bookings;
- updating guest information during check-in;
- coordinating with an external booking platform.

For the selected process, identify:

- One risk point during data entry.
- One risk point during system-to-system transfer.
- One risk related to human behaviour.
- One moment where escalation or reporting might be required.

For each identified risk point, briefly describe:

- what could go wrong;
- what the potential consequence would be;
- one preventive action.

After 10–15 minutes, each group presents their findings.

Reflection & Discussion

01

What is a digital risk point, and why do risk points increase in digital processes?

02

Give one example of a risk during payment processing and one correct employee action.

03

Why is analysing risk across the full customer journey more effective than reviewing each step separately?

2. Secure Customer Data Management

Secure management of customer data is a **core operational responsibility** in tourism organisations. Reservation records, identity details, contact information, and payment-related data are processed daily through CRM systems and interconnected platforms. These systems enable service efficiency and personalisation, but they also concentrate structured personal data. If controls are weak, they can become high-impact exposure points.

Effective data protection begins with purposeful collection. Organisations should collect only information necessary to deliver the service and meet legal obligations. Collecting additional fields for convenience increases the volume of sensitive data stored and therefore increases potential impact if systems are compromised.

This principle, known as data minimisation, reduces risk in practical terms:

- fewer sensitive data elements stored;
- reduced breach impact;
- simplified monitoring and oversight;
- lower compliance exposure in case of incident.

Limiting data collection is not a technical restriction — it is a strategic risk management decision.

The principle of data minimisation is explicitly established in Article 5(1)(c) of the General Data Protection Regulation (GDPR), which requires that personal data be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (Regulation (EU) 2016/679)¹⁰.

Access Control and System Safeguards

After data collection, operational safeguards must ensure that only authorised staff can access or process customer information.

Core controls include:

¹⁰ European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>

- role-based access permissions aligned with job functions (Access is granted based on **job titles** (e.g., HR, Finance) rather than individuals, ensuring users only see tools relevant to their specific department);
- application of the least-privilege principle (Users are given the **bare minimum** access levels needed to perform their tasks, strictly limiting the potential damage from a compromised account);
- multi-factor authentication (MFA) (Requires **two or more proofs** of identity (e.g., a password plus a phone code) to log in, making stolen passwords useless on their own);
- encryption of sensitive data at rest and in transit (Scrambles data into unreadable code both while it is **stored** on a disk and while it is **moving** across the internet or a network);
- logging and monitoring of access, exports, and modifications (Creates a **digital paper trail** of who viewed, changed, or moved data, allowing security teams to spot and investigate suspicious activity in real-time.).

In CRM environments, monitoring is particularly important. Indicators such as unusual login times, repeated data exports, bulk record modifications, or access from unexpected locations may signal misuse or compromise. Early detection significantly limits escalation.

Secure access management also requires attention during staff changes, shift transitions, and role modifications. Delayed removal of permissions or shared credentials weakens traceability and increases exposure.

Operational Behaviour and Escalation

Technical safeguards alone are insufficient. Secure data management depends equally on disciplined employee behaviour.

Staff should:

- avoid storing payment data in free-text fields or internal notes;
- avoid exporting data unless operationally necessary;
- follow formal procedures for corrections and deletions;
- log out of systems when not in use;
- question unusual access requests.

As established in earlier sections, independent corrective action during suspected incidents may destroy audit trails and complicate regulatory assessment. Escalation through defined channels ensures evidence preservation and coordinated decision-making.

Timely escalation allows IT and management to assess containment measures and determine whether notification obligations apply. Early action directly reduces operational disruption and reputational damage.

Retention, Deletion, and Secure Integration

Data security extends beyond access and monitoring. Retaining data longer than necessary increases exposure without operational benefit. Clear retention and deletion policies should define:

- retention periods for booking and reservation data;
- anonymisation or tokenisation of payment-related information;
- authorisation procedures for deletion;
- documentation of deletion actions.

Secure integration with payment platforms is equally important. CRM systems should avoid storing full card details unless strictly necessary and compliant with payment security standards. Where possible, tokenisation or secure gateways reduce concentration of financial risk.

Testing incident response procedures — including cooperation with IT and external providers — completes the secure data management cycle. Detection, containment, documentation, and communication must function together.

Together, these measures create a structured data protection framework: controlled collection → restricted access → monitored usage → defined retention → documented deletion.

Practical Activity: CRM Risk Review Exercise

Learners analyse a simplified CRM structure containing: guest contact details, scanned identity documents, full payment card number, internal notes, marketing history, archived booking data for ten years.

1. Identify which data elements represent highest exposure.
2. Identify which data elements may exceed operational necessity.
3. Propose one improvement in access control.

4. Propose one improvement in retention policy.
5. Explain which change would most reduce overall risk and why.

Going Beyond

Advanced assessment of data minimisation involves structured review of:

- mandatory versus optional data fields;
- automated data feeds and external integrations;
- retention schedules and deletion verification;
- pseudonymisation or tokenisation practices;
- alignment between operational need and stored information.

Prioritising corrections where unnecessary data is retained longest delivers the greatest reduction in exposure.

Reflection & Discussion

01

What is data minimisation and why is it a strategic risk management measure?

02

Name two operational safeguards that protect CRM data and explain how one reduces impact.

03

Going Beyond: How would you prioritise improvements in a CRM system with excessive stored data?

3. Payment, Fraud and Booking Scams

Payments and bookings represent high-value stages in digital tourism processes because they directly involve financial transactions and customer trust. Unlike general data exposure, payment incidents often result in immediate and measurable harm: financial loss, chargebacks, reputational damage, and increased operational workload.

Fraud in tourism frequently targets points where money moves or where refundable obligations exist. The combination of remote transactions, time pressure, and cross-border bookings increases vulnerability.

Common Fraud Types in Tourism

Several fraud patterns regularly appear in tourism operations:

- **Card-not-present (CNP) fraud** – stolen card details used without physical card verification;
- **Stolen or compromised accounts** – attackers gain access to booking profiles and modify reservations;
- **Booking scams using false identities** – fraudulent reservations made to manipulate pricing or cancellation policies;
- **Business Email Compromise (BEC)** – attackers impersonate suppliers or partners to redirect payments;
- **Refund manipulation** – false refund requests exploiting operational confusion.

Fraudsters rarely rely on technical sophistication alone. Many attacks exploit urgency, trust, or procedural shortcuts.

Warning Signals and Operational Indicators

Effective fraud detection depends on recognising patterns rather than isolated anomalies. Typical warning signals in tourism payment and booking environments include:

- unusually high booking amounts;
- multiple bookings in rapid succession from the same account or IP address;
- mismatched billing and contact information;
- repeated failed authorisations;
- urgent requests to change payment details;
- pressure to bypass normal verification procedures.

Individually, these signals may reflect operational irregularities rather than confirmed fraud. However, their analytical value increases significantly when evaluated in combination.

To support structured assessment, fraud indicators can be categorised into three analytical layers:

- **Isolated anomalies** – single irregular transaction or mismatch without pattern evidence
- **Pattern anomalies** – repeated irregularities from the same IP, device, account, or payment method
- **Coordinated fraud signals** – compound indicators such as high-velocity bookings combined with identity mismatch and urgency language

Higher-layer indicators require immediate escalation, as they typically signal structured or organised fraud rather than accidental irregularities. Prioritising compound patterns significantly improves detection efficiency and reduces unnecessary operational disruption.

Operational Response to Suspicious Transactions

When a payment or booking appears suspicious, immediate action should follow structured procedures rather than informal judgement.

Staff should:

- pause fulfilment of the transaction;
- avoid processing refunds or changes without verification;
- request additional confirmation through approved channels;
- escalate to finance, IT, or management according to defined procedures;
- document actions taken.

Attempting to “solve the problem quickly” under operational pressure can increase exposure. Structured escalation protects both customers and the organisation.

Prevention Controls

Fraud prevention combines technical safeguards and behavioural discipline.

Key controls include:

- **Secure payment gateways**, which ensure encrypted processing and reduce exposure of card data within internal systems;
- **3-D Secure (3DS) authentication**, which adds an additional verification step to confirm the cardholder’s identity during online transactions;
- **Transaction monitoring and velocity rules**, which detect unusual patterns such as rapid repeated bookings, sudden high-value transactions, or repeated failed authorisations;
- **Separation of duties in payment approval**, where different staff members authorise and process financial changes to reduce internal and external fraud risk;
- **Clear escalation thresholds**, defining when a transaction must be reviewed by management or IT rather than processed automatically;
- **Regular fraud awareness training**, reinforcing recognition of pressure tactics, impersonation attempts, and booking anomalies.

No single control is sufficient. Layered safeguards reduce both likelihood and impact.

Regulatory Context

Fraud prevention in payment processing is reinforced by European regulatory requirements. **Directive (EU) 2015/2366 on payment services (PSD2)** ¹¹ introduced the obligation for Strong Customer Authentication (SCA) for electronic payments. SCA requires at least two independent authentication factors and is commonly implemented through mechanisms such as 3-D Secure (3DS).

For tourism organisations, this means that secure payment verification is not merely a best practice, but part of a regulated framework aimed at reducing online fraud and protecting consumers within the European Union.

Scenario

The Incident: An email arrives from a long-term supplier stating that their bank account has changed and requesting urgent update of payment details. The message stresses that failure to update immediately may result in service interruption for an upcoming event.

"If you don't update this now, we won't deliver the food for tonight's wedding banquet!"

Group Task

1. Warning indicators in the message.
2. Risks if the request is processed without verification.
3. Correct verification steps.
4. Escalation procedures required.
5. Which control could have prevented or limited the risk.

Going Beyond

Fraud pattern analysis involves identifying which indicators most strongly predict organised or automated attacks. High-velocity bookings, sudden high-value transactions, repeated failed authorisations, and IP or device inconsistencies often signal structured fraud activity.

¹¹ European Union. (2015). *Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*. Official Journal of the European Union.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366>

Prioritising monitoring at these high-impact indicators improves detection efficiency and reduces unnecessary operational friction.

Reflection & Discussion

01

Name two common payment fraud types in tourism and one indicator for each.

02

What is the correct immediate response when a transaction appears suspicious?

03

Why can operational pressure increase fraud risk?

04

Going Beyond:
Which fraud indicators should be prioritised in monitoring systems, and why

4. Scenario Exercise: Suspicious Payment

Practical Activity

Objective: Apply fraud detection hierarchy and structured escalation procedures.

Format: Scenario-based group analysis

Estimated Duration: 30–40 minutes

Scenario Description:

A member of the accounting department receives an email from a long-term supplier (e.g., laundry service or food distributor). The request appears plausible. The supplier relationship is genuine, and the timing aligns with scheduled payment.

The message states:

"Dear Accounting, please find the updated bank details for our upcoming monthly invoice. Our previous account is being closed due to an audit. Please update your records immediately and confirm when the payment for next week is scheduled. Failure to update may result in a service suspension."

Attachment: [New_Bank_Details_and_Invoice.pdf](#)

Group Discussion: How to React?

Learners analyse the scenario in small groups, focusing on three structured stages of assessment: identifying the risk point, recognising warning indicators, and defining the correct operational response.

Step 1: Identifying the Risk Point

Discuss:

- Why is the accounting department a high-value target?
- What operational authority makes this department particularly vulnerable?

Key consideration:

Accounting teams have direct authority to modify payment records and execute financial transfers. Compromise at this point leads to immediate financial harm rather than delayed or indirect consequences.

Step 2: Identifying Warning Indicators

Learners identify potential red flags, such as:

- urgency and pressure language;
- request to change established payment details;
- threat of service disruption;
- unexpected account closure explanation;
- attachment requesting action.

Although the email may not contain malicious links, the risk lies in procedural manipulation rather than malware.

This scenario reflects a common fraud type: **Business Email Compromise (BEC)**.

Step 3: Structured Response

Learners determine the correct response sequence.

Appropriate actions include:

- pausing payment modification;

- refraining from updating bank details immediately;
- verifying the request through an independent channel (e.g., calling the supplier using an existing verified contact number);
- escalating internally according to financial control procedures;
- documenting the interaction.

Verification must occur through a separate communication channel. Using contact information provided in the suspicious email does not constitute independent verification.

Learners should also consider:

- at what point management or IT should be informed;
- how documentation protects both the employee and the organisation;
- which existing control (e.g., separation of duties) should prevent this scenario.

5. First 24 Hours After a Data Breach

When a **data breach** is detected, the first 24 hours are critical. Early decisions influence the scale of impact, regulatory exposure, operational disruption, and reputational damage. Delays or uncoordinated actions during this period can significantly increase harm.

The immediate priority is **containment**. Containment involves isolating affected systems, stopping unauthorised access, and preventing the breach from spreading further. If containment is delayed, additional data may be exposed, system recovery becomes more complex, and financial and reputational costs increase.

However, containment must occur in a controlled and documented manner.

Immediate Priorities in the First 24 Hours

The initial response should focus on the following actions: identifying affected systems and data categories, isolating compromised accounts or systems, preserving logs and evidence, notifying internal escalation contacts, and documenting all actions taken. Preserving evidence is particularly important.

Uncoordinated attempts to “clean up” systems may destroy forensic traces, making investigation more difficult and potentially increasing regulatory risk.

As previously highlighted, uncoordinated intervention may unintentionally expand the scope of the breach or compromise forensic evidence. In the first 24 hours, disciplined escalation and controlled containment are essential to limit regulatory and reputational exposure.

Documentation and Audit Trail

Accurate documentation during the first 24 hours is essential. A clear timeline should record:

- **when** the breach was detected;
- **who** reported it;
- **what systems** were affected;
- **what containment** actions were taken;
- **who** authorised decisions.

This audit trail supports investigation, regulatory reporting, and post-incident learning. It also protects employees by demonstrating that procedures were followed.

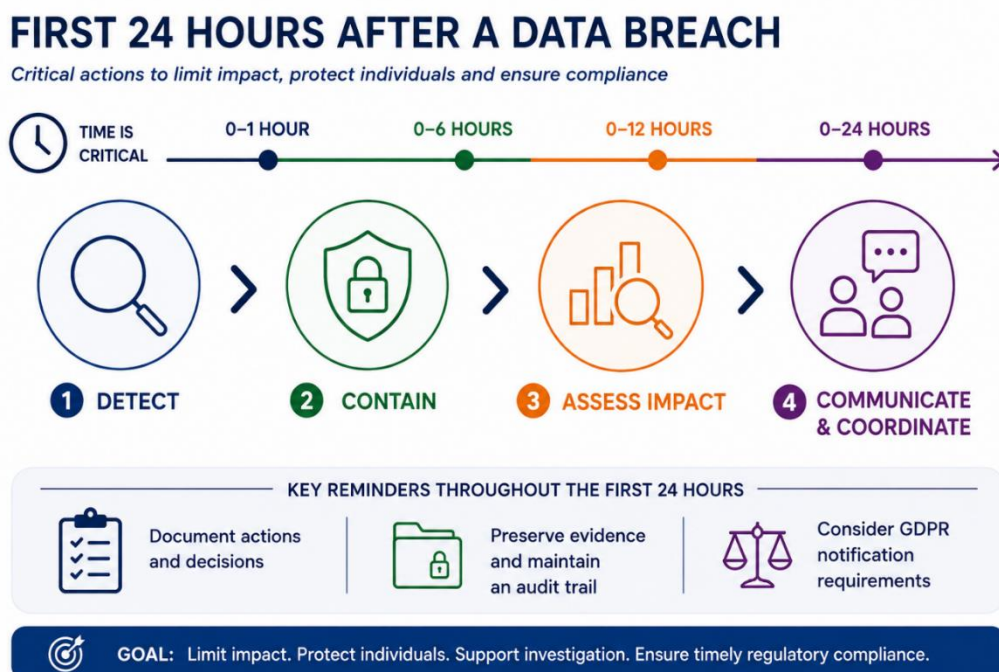


Figure 3: Key response phases during the first 24 hours after a data breach

Regulatory Considerations

Under Article 33(1) of the General Data Protection Regulation (GDPR, 2016), organisations must notify the competent supervisory authority within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in risk to individuals.

“In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (...) unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.” (GDPR, 2016, Art. 33)

In addition, **Article 34** requires organisations to **communicate the breach directly to affected individuals** when it is likely to result in a high risk to their rights and freedoms.

This means that during the first 24 hours, organisations must not only contain the breach, but also conduct a **structured preliminary impact assessment** to determine regulatory and operational consequences. Specifically, they must evaluate:

- whether personal data is involved;
- the level of risk to affected individuals;
- whether supervisory authority notification is required;
- whether direct communication to individuals may be necessary.

Early and structured assessment reduces both regulatory exposure and reputational harm.

To support this evaluation, organisations should apply a rapid impact scoring framework based on defined criteria:

1. Sensitivity of data involved (identity, payment, health, travel patterns)
2. Volume of records potentially affected
3. Criticality of affected systems (core operations vs auxiliary systems)
4. Potential regulatory exposure

Applying a simple 1–3 scoring scale per category enables defensible prioritisation, supports proportionate containment measures, and strengthens the legal basis for supervisory notification decisions within the GDPR 72-hour timeframe.

Communication and Reputation

During the first day, organisations should prepare **clear internal and external communication plans**. Communication must be accurate, factual, and coordinated. Premature or speculative statements can increase confusion and reputational harm.

Digital incidents affect customers, staff workload, and organisational stability. Awareness of these broader impacts reinforces why structured, timely action is essential.

Scenario: 24-Hour Response Mapping

A staff member reports that an unauthorised user accessed the reservation system overnight. Several guest records may have been viewed or exported.

In small groups, learners:

- Define the first three actions that should be taken.
- Identify which roles must be informed.
- Determine whether regulatory notification may be required.
- Outline what must be documented within the first 24 hours.

Groups justify their decisions based on impact and risk.

Going Beyond

Responding quickly is essential, but acting without structure can increase exposure. Rushed actions may overlook legal obligations or destroy evidence. Conversely, excessive caution may allow the breach to spread.

An effective response balances speed with structured procedure. Clear escalation paths, predefined roles, and documented decision-making enable organisations to act rapidly while meeting regulatory and operational requirements.

Reflection & Discussion

01

What is the first priority during the first 24 hours after a data breach, and why?

02

Why must employees report incidents immediately rather than attempting to fix them independently?

03

What information should be documented during the initial response phase?

6. Cooperation with IT and External Providers

Effective cooperation with IT teams and external providers is essential in digitally interconnected tourism environments. Reservations, payments, CRM systems, cloud services, and booking platforms are often managed through third-party solutions. When incidents occur, resolution rarely depends on one department alone.

Digital risk in tourism frequently extends beyond organisational boundaries. Weaknesses in supplier systems, misconfigured integrations, or delayed communication can increase impact across the entire ecosystem.

Internal Cooperation

When a digital issue is detected, structured cooperation between operational staff and IT teams is critical.

Operational staff are typically the first to observe irregularities. However, technical containment requires IT expertise. Effective cooperation depends on clear communication and accurate reporting.

When reporting an incident, staff should provide:

- time and date of detection;
- system involved;
- user account affected;
- description of unusual behaviour;
- actions already taken.

Incomplete or vague reporting delays containment and complicates investigation.

Clear role definitions prevent confusion. Operational staff report and preserve information; IT investigates and isolates systems; management coordinates decisions; compliance or legal teams assess regulatory obligations.

Uncoordinated intervention by non-technical staff can unintentionally expand exposure or compromise evidence.

Cooperation with External Providers

Many tourism organisations rely on cloud-based PMS providers, online travel agencies (OTAs), payment gateways, CRM vendors and outsourced IT services. If an

incident involves externally hosted systems, timely communication with providers is essential. Providers may need to:

- isolate affected servers;
- disable compromised accounts;
- provide system logs;
- confirm breach scope;
- support regulatory reporting.

Delayed notification to providers may prolong exposure and increase operational downtime.

Clear contractual agreements should define:

- security responsibilities;
- incident reporting timelines;
- access rights;
- data protection obligations;
- audit rights and verification mechanisms.

Supplier governance is therefore a preventive measure, not merely a contractual formality.

Supply-Chain Risk and Regulatory Context

Under the NIS2 framework and related European cybersecurity guidance, organisations must manage risks not only within their own systems but also across their supply chains.

Tourism businesses relying on interconnected digital providers must assess:

- which suppliers process personal data;
- which suppliers have direct system access;
- what security controls are contractually required;
- how incidents are communicated and escalated.

A failure in a third-party provider may quickly escalate into a multi-organisation incident. Proactive supplier oversight reduces systemic risk.

Documentation and Continuous Improvement

Cooperation should be documented at every stage. Records of communication with IT and external providers support:

- regulatory compliance;
- incident review;
- identification of procedural weaknesses;
- future risk reduction.

Post-incident evaluation should include analysis of communication effectiveness and response speed. Digital resilience depends on coordination, not individual action.

Reflection & Discussion

01

Why is accurate reporting to IT essential during a digital incident?

02

What information should operational staff provide when escalating an issue?

03

Why does supplier governance reduce systemic risk?

7. Advanced Technologies in Digital Tourism Security

Digital tourism environments increasingly rely on advanced technologies to **strengthen data protection, identity verification, and transaction integrity**. While operational discipline remains essential, certain technological solutions can significantly reduce systemic risk when implemented correctly.

Advanced security technologies do not replace responsible behaviour. Instead, they reinforce existing controls and reduce the likelihood that human or technical weaknesses escalate into major incidents.

Blockchain and Data Integrity

Blockchain is a distributed ledger technology designed to enhance data integrity and traceability in multi-party digital environments. By linking transactions sequentially in a tamper-evident structure, it increases transparency and accountability across interconnected systems.

In tourism ecosystems involving multiple actors—such as hotels, OTAs, and payment providers—blockchain may support:

- integrity verification of booking records,
- tamper-resistant transaction logging,
- strengthened trust in supplier interactions.

Industry analyses, such as Mize (2023)¹², further suggest that blockchain may reduce reconciliation inefficiencies and enhance transactional transparency within travel distribution networks.

Its primary security contribution lies in integrity protection within shared digital environments. However, blockchain does not address behavioural vulnerabilities such as phishing, credential misuse, or weak access control. Its effectiveness therefore depends on broader governance maturity, structured access management, and proportional implementation based on operational necessity rather than technological trend adoption.

Secure Digital Identity and Strong Authentication

Identity management remains one of the most critical control points in digital tourism. Stolen or misused credentials frequently serve as entry points for fraud and data breaches.

Secure identity systems may include:

- multi-factor authentication (MFA);
- federated identity solutions;
- single sign-on with conditional access controls;
- biometric verification in high-risk transactions.

Strong identity verification reduces account takeover risk and limits lateral movement within interconnected systems. It supports the Zero Trust principle introduced earlier: no implicit trust, continuous verification.

In ecosystems where hotels, OTAs, and payment providers interact, identity assurance significantly reduces cross-platform risk.

¹²Ref. Mize. (2023). *Unlocking the Potential of Blockchain Technology in Travel*.
<https://mize.tech/blog/unlocking-the-potential-of-blockchain-technology-in-travel/>

System Interconnection and Ecosystem Security

Advanced technologies are particularly relevant in environments where multiple digital actors interact. Tourism platforms often involve:

- property management systems (PMS);
- online travel agencies (OTAs);
- payment processors;
- marketing platforms;
- cloud hosting providers.

Technological safeguards such as API security controls, encryption standards, and automated monitoring systems strengthen trust between interconnected systems. However, technological complexity may introduce new dependencies. Poor configuration or insufficient oversight can offset intended benefits.

Cost-Benefit and Risk-Based Evaluation

Adopting advanced security technologies should be the result of careful assessment rather than a reaction to isolated incidents or market trends. Introducing such technologies involves more than acquiring new software or tools. It requires financial resources, integration with existing systems, staff training, and adjustments to daily operational procedures. In many cases, organisations must also review internal responsibilities and governance arrangements to ensure that new controls function effectively within existing workflows.

A cost-benefit assessment should examine both immediate and long-term effects. This includes potential reduction in fraud losses and service disruption, improvements in compliance posture, and strengthened customer trust. The aim is not technological complexity, but proportional and demonstrable improvement in security resilience.

Not all solutions are equally appropriate for every organisation. Smaller operators may achieve substantial protection by reinforcing identity controls and secure payment processes, while larger and more interconnected organisations may justify more advanced technologies where system-wide integrity and interoperability are strategic concerns.

Risk-based prioritisation helps ensure that security investments remain aligned with organisational exposure, operational dependency, and overall risk profile.

Human Factor Remains Central

Even the most advanced technologies cannot compensate for weak password practices, failure to report anomalies, misuse of credentials, or procedural shortcuts taken under operational pressure. These human behaviours frequently serve as entry points for incidents, regardless of how sophisticated the technical safeguards may be.

Technology strengthens organisational resilience only when it is supported by disciplined operational conduct. Secure systems require responsible users. Identity controls, monitoring tools, and encryption mechanisms reduce exposure, but they do not eliminate the need for vigilance and adherence to procedures.

Digital security in tourism is therefore both technical and organisational. Sustainable resilience depends on the interaction between structured technological controls and consistent, responsible behaviour across all operational roles.

This principle also applies to the **growing use of Artificial Intelligence (AI) tools in tourism**. While AI can support content creation, customer communication, marketing, and operational tasks, it should be **used responsibly** (e.g. avoiding the upload of personal or sensitive customer information into public AI systems) **and in accordance with organisational policies, data protection requirements, and applicable regulations**. Staff should verify AI-generated outputs, use approved AI services where available, and ensure that human judgement remains central to decision-making processes.

Going Beyond

Learners analyse how advanced security technologies align with broader strategic frameworks, including Zero Trust principles, supply-chain resilience expectations under NIS2, long-term digital trust building, and the need for scalability across interconnected tourism ecosystems.

They evaluate which technological approach would most effectively strengthen resilience at the ecosystem level, rather than focusing solely on protection of individual systems.

Reflection & Discussion

01

What is the primary security benefit of blockchain technology?

02

Why is identity management central to reducing digital risk?

03

Why must technology investment be risk-based rather than trend-driven?

04

Going Beyond: Which advanced control would most improve systemic resilience in a multi-partner tourism ecosystem?

8. Reflection & Consolidation

Individual Reflection

Learners individually prepare short written responses addressing the following questions:

1. Which stage of the digital tourism process in your organisation carries the highest digital risk, and why?
2. Which type of human behaviour represents the greatest vulnerability?
3. Which single improvement would most effectively reduce risk in your workplace?

Responses should demonstrate understanding of operational, behavioural, and regulatory dimensions of digital risk.

Small Group Analysis

In groups of three to four, learners compare their reflections and identify:

- one shared high-risk process;
- one common behavioural vulnerability;
- one improvement that could realistically be implemented.

Each group prepares a short summary explaining their reasoning. Their analysis should be structured using the following criteria:

- operational, financial, and reputational impact;

- likelihood of occurrence;
- potential regulatory implications.

Groups present their conclusions briefly and justify prioritisation decisions.

Scenario: A Busy Weekend Escalation

It is the beginning of peak tourist season. The hotel is fully booked due to a large international conference in the city.

The accounting department receives an urgent email from a long-term supplier requesting an immediate change of bank details. The message cites an “audit issue” and warns that failure to update payment information may delay deliveries for the event.

Due to operational pressure and limited staff availability, the change is processed without additional verification.

Two days later, IT detects unusual login activity in the CRM system. Several guest records appear to have been accessed outside normal working hours, and it is unclear whether data has been exported.

At this stage, the supplier contacts the organisation asking why payment has not been received. Simultaneously, front desk staff report guest complaints about suspicious refund emails. With multiple irregularities emerging at once, management requests urgent clarification and an immediate assessment of potential impact.

The organisation now faces a potentially connected payment fraud and data breach during peak season.

Group Task

In small groups, learners analyse the situation and outline:

1. What should be the first immediate action?
2. Which internal roles must now be involved?
3. Which systems should be checked or isolated?
4. What information must be documented within the first 24 hours?
5. Does this situation potentially trigger GDPR notification obligations?
6. Which earlier control (process, behaviour, or technology) might have prevented escalation?

Groups should justify their decisions by considering operational impact, financial exposure, regulatory risk, and reputational consequences.

Reflection Focus

Learners should evaluate how operational pressure influenced decision-making and how small procedural deviations accumulated into a larger incident. Particular attention should be given to the importance of early verification, structured escalation, and coordinated cooperation with IT teams and suppliers.

The discussion should emphasise how disciplined processes protect both staff and the organisation, especially during high-pressure operational periods.

2.3 Simulations and Digital Crisis Management

At the end of this sub-unit, students will be able to react correctly in digital emergencies, communicate clearly and responsibly, avoid escalation of damage and support recovery actions.

- Types of digital incidents: phishing and reservation fraud, ransomware, DDoS, data leaks, account takeovers
- Communication hierarchy: internal staff, customers, authorities (DPA), media
- Post incident recovery: system restoration and trust rebuilding
- Psychological pressure during digital crisis

Suggested practical activity:

- Case study 1: ransomware attack on a hotel PMS.
- Case study 2: Booking platform phishing campaign.
- Workshop: communication plan for data leak crises.

1. Types of Digital Incidents in Tourism

Digital incidents occur when systems handling **reservations, payments, or customer data** are disrupted, misused, or compromised. Most incidents follow a clear cause-and-effect logic: a vulnerability or human error enables access, disruption, or manipulation, which then produces operational, financial, legal, or reputational consequences.

Recognising incident categories allows staff to respond proportionally rather than react emotionally.

Common incident types include:

- **Data breaches** – unauthorised exposure of personal or payment data, often leading to regulatory obligations and reputational harm.
- **System outages** – unavailability of critical platforms due to technical failure or attack, causing service disruption and revenue loss.
- **Payment incidents** – fraudulent transactions, incorrect charges, or chargebacks affecting financial stability.
- **Unauthorised access** – access to systems or data without proper authorisation, increasing risk of manipulation or leakage.

- **Reputational manipulation or disinformation** – coordinated misinformation affecting trust and booking behaviour.

Each incident type affects stakeholders differently. Customers may experience financial or privacy harm; staff may face operational pressure and reporting obligations; management must address regulatory and reputational exposure.

Effective response begins with disciplined reporting, structured escalation, and controlled communication.

Going Beyond

Classifying incidents by **severity and impact scope** supports proportional prioritisation. Low-severity incidents may be contained locally, while high-severity incidents involving sensitive data, systemic disruption, or regulatory exposure require immediate escalation, senior oversight, and coordinated crisis management.

However, severity should not be assessed statically. Digital incidents in tourism environments often evolve progressively through identifiable escalation stages:

1. **Anomaly detection** – minor irregularity or unusual system behaviour observed
2. **Local compromise** – limited system, account, or device affected
3. **Lateral movement** – spread across interconnected systems or user accounts
4. **Operational disruption** – service interruption, financial loss, or booking failure
5. **Regulatory and reputational escalation** – supervisory authority involvement, customer notification, public exposure

Recognising these escalation stages enables earlier intervention, limits systemic spread, and supports defensible regulatory decision-making. Proactive identification at the anomaly or local compromise stage significantly reduces operational and reputational damage.

Reflection & Discussion

01

Name two types of digital incidents and one possible consequence of each.

02

Why is structured reporting essential during an incident?

03

Going Beyond: How does severity classification improve decision-making?

2. Psychological Pressure in Digital Crises

Digital crises rarely unfold in calm conditions. Stress, uncertainty, and time pressure reduce attention and increase the likelihood of procedural shortcuts. Cognitive overload may cause staff to skip verification steps or act prematurely, potentially expanding the impact of the incident.

Research in human factors and cybersecurity consistently demonstrates that stress, cognitive overload, and time pressure significantly increase the likelihood of procedural errors during incident response, reinforcing the need for structured escalation and predefined roles¹³.

The failure to escalate early — as discussed in Sub-units 2.1 and 2.2 — is frequently a systemic trigger in crisis escalation. Under psychological pressure, individual corrective attempts often undermine structured response and increase long-term impact.

Structured procedures mitigate these risks. Clear escalation pathways, defined responsibilities, and short decision checklists reduce ambiguity. A named incident manager centralises coordination and limits contradictory actions.

Practical stabilisation measures include:

- pause-and-verify protocols before irreversible actions;
- rehearsed reporting routines;
- visible leadership support encouraging early escalation;
- post-incident debriefs to reinforce learning.

¹³ European Union Agency for Cybersecurity (ENISA). (2019). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

Crisis resilience depends as much on behavioural discipline as on technical capacity.

Going Beyond

Leaders should establish decision thresholds defining when immediate escalation is mandatory. Decision aids such as simplified RACI models or escalation matrices support consistent action under stress. Effective leadership balances speed with evidence preservation and staff wellbeing.

Reflection & Discussion

01

Identify two psychological factors that increase error risk during a crisis.

02

Why is escalation preferable to individual problem-solving in high-pressure situations?

03

Going Beyond: How can leadership structure decision-making to maintain both speed and accuracy?

3. Case Study 1 – Ransomware Attack on a Hotel Property Management System (PMS)

Practical Activity

Objective: Demonstrate coordinated incident response under operational pressure.

Format: Role-based group simulation

Estimated Duration: 60–90 minutes

This activity enables learners to apply crisis management principles in a simulated ransomware scenario. Participants practise structured escalation, coordinated decision-making, regulatory assessment, and communication under operational pressure.

A mid-sized city hotel is hit by a ransomware attack overnight. When the morning shift arrives, staff are unable to access the Property Management System (PMS). Reservation records are encrypted, automatic payments have failed, and card pre-authorisations cannot be verified. Check-in queues begin forming within minutes.

Initial investigation reveals that the attack originated from a phishing email opened during the night shift. The malware executed on a workstation connected to the PMS

network. Because network segmentation was insufficient, the malicious code spread laterally to shared backup systems, rendering them temporarily unusable.

The operational impact is immediate and escalating. Front desk staff revert to manual registration procedures. Guests express frustration over delays. Finance teams cannot confirm transactions. Management must decide whether to shut down external access entirely, potentially worsening operational disruption.

Within hours, the hotel is confronted with multiple, interconnected layers of exposure. Core booking operations become paralysed, disrupting check-ins and reservations. Financial losses begin to accumulate due to cancelled bookings and chargebacks. At the same time, if the integrity of personal data has been compromised, regulatory notification obligations may arise. Reputational damage escalates rapidly as guests share complaints and concerns online, amplifying the impact beyond the immediate operational failure.

Containment requires rapid isolation of infected systems, restriction of network access, engagement of external forensic specialists, and verification of clean backups before restoration. Recovery extends over several weeks and demands coordinated technical, operational, and communication efforts.

Initial Situation Assessment

Learners work in small groups. They must:

- identify immediate operational, financial, regulatory, and reputational risks;
- determine whether the incident may qualify as a potential personal data breach;
- define the first operational action to be taken within the first 30 minutes.

Groups present short justifications based on impact and escalation logic.

Role-Based Crisis Coordination

Learners are assigned specific organisational roles:

- Operations Manager
- IT Lead
- Finance Manager
- Communications Lead
- Compliance / Data Protection Officer

Each group must agree on:

- immediate containment measures;
- system isolation decisions;
- whether external forensic support is required;
- whether regulatory risk assessment should begin;
- internal communication priorities.

Each role briefly outlines its primary concerns and decision priorities. The objective is to demonstrate coordinated action rather than isolated responses.

Escalation Under Public Pressure

The trainer introduces additional developments:

- Media reports suggest “system failure at the hotel”.
- A guest publicly questions whether payment data has been compromised.

Groups must decide:

- what information can be communicated immediately;
- what must remain under investigation;
- who acts as spokesperson;
- whether external notification procedures should begin.

Decisions must balance transparency with legal and forensic considerations.

Root Cause and Preventive Strategy

Groups conduct a short-structured review:

- What failure enabled the incident to escalate?
- Which technical control would most reduce recurrence?
- Which behavioural or procedural improvement is required?
- Which supplier or governance element contributed to exposure?

Groups prioritise corrective measures based on systemic risk reduction.

Going Beyond

A structured root cause analysis identifies three systemic weaknesses: successful phishing exploitation, inadequate network segmentation, and backups located within the same accessible environment. Corrective priorities include:

- strengthened email filtering and phishing awareness testing;
- improved network segmentation to prevent lateral spread;
- implementation of offline or immutable backups;
- reinforced escalation protocols to ensure earlier detection and reporting.

Applying a structured review method (incident timeline → root cause mapping → prioritised remediation plan) ensures that lessons translate into measurable resilience improvements rather than temporary fixes.

4. Case Study 2 – Booking platform phishing campaign

Practical Activity

Objective: Explore how a tourism business should respond when guests become targets of a phishing campaign.

Format: Group discussion and problem-solving exercise

Estimated Duration: 45–60 minutes

This activity enables learners to analyse a phishing incident affecting guests through a trusted booking platform. Participants practise risk assessment, customer communication, coordination with external partners, and response planning.

A small hotel starts receiving calls from guests who have received messages asking them to make an additional payment to confirm their reservation. The messages appear to come from a well-known booking platform and include a link to a payment page.

Several guests follow the instructions and enter their payment details before realising that the messages are fraudulent.

The hotel contacts the booking platform and learns that attackers may have gained access to one of the platform accounts used to communicate with guests. As more reports arrive, guests begin posting warnings on social media and review websites. Hotel staff are unsure how much information they should provide and how they should respond to concerned customers.

Initial Assessment

Working in small groups, discuss:

- What are the main risks for guests?
- What are the main risks for the hotel?
- What information is already available?
- What additional information is needed before decisions can be made?
- What should be done during the first few hours after the incident is identified?

Managing the Situation

Your group represents the hotel management team.

Discuss and agree on:

- How guests should be informed about the incident?
- What advice should be provided to affected guests?
- Who should communicate with the booking platform?
- Whether a public statement should be issued?
- What actions can help maintain customer trust.

Prepare a short action plan and explain your decisions.

Review and Prevention

After discussing the scenario, consider the following questions:

- Why were guests likely to trust the messages?
- Which warning signs might have indicated that the messages were fraudulent?
- What measures could help prevent similar incidents in the future?
- How can tourism businesses help guests recognise phishing attempts?

Going Beyond

This case shows that cyber incidents do not always begin inside an organisation's own systems. Tourism businesses often rely on booking platforms, payment providers, and other digital partners. When one part of this ecosystem is affected, customers may still associate the problem with the accommodation provider.

Measures that may reduce risk include:

- enabling multi-factor authentication for platform accounts;

- regularly reviewing account activity;
- providing staff with phishing awareness training;
- informing guests about official payment procedures;
- establishing clear communication procedures for digital incidents.

The scenario highlights the importance of customer communication, third-party platform security, and maintaining trust during a digital incident.

5. Crisis Communication

Why Communication Determines Crisis Outcome

During a digital incident, communication is not secondary to technical response; it is a central element of crisis management. The way information is shared influences containment speed, regulatory compliance, stakeholder confidence, and long-term organisational trust. Poorly structured or informal messaging can quickly intensify a technical incident into a broader reputational crisis.

When communication lacks coordination, internal confusion increases. Staff may receive inconsistent instructions, duplicate actions may occur, and premature statements may reach guests or the media. This not only slows containment but may also increase legal exposure and damage public trust. For this reason, crisis communication must be disciplined, proportionate, and strategically coordinated.

Core Communication Principles

Effective crisis communication in tourism environments is based on five principles:

1. **Accuracy before speed** – verify facts before public disclosure.
2. **Single point of authority** – designate one spokesperson.
3. **Internal alignment first** – ensure staff understand the situation before external messaging.
4. **Transparency without speculation** – communicate what is known, avoid assumptions.
5. **Documented communication trail** – retain records for legal and regulatory review.

Internal Communication Structure

Immediately after an incident is identified, **relevant teams** should receive a concise factual briefing. This briefing should clarify **what is confirmed, what remains under investigation, what immediate actions are required, and who is authorised to communicate externally**.

Clear internal communication reduces uncertainty and prevents unsanctioned actions. In high-pressure situations, staff may feel compelled to “fix” issues independently or respond informally to guest enquiries. Structured internal coordination mitigates these risks and protects both staff and organisational credibility.

External Communication to Guests

Guest communication must balance clarity, empathy, and factual precision. Messages should explain the **operational impact of the incident**, outline **immediate steps being taken**, and provide **practical guidance or support channels**. The tone should remain calm and responsible, avoiding defensive language or premature conclusions.

Speculative statements can create additional legal and reputational risk, particularly in cases where personal data integrity has not yet been confirmed. Consistency across communication channels is therefore essential. Contradictory updates from different departments can significantly undermine trust.

Digital Accessibility in Crisis Communication

Crisis communication strategies must **ensure that information reaches all guests, including those with visual, hearing, or cognitive impairments**. During digital incidents, reliance on a single communication channel may exclude certain groups, particularly if systems are disrupted.

Accessible communication requires the use of multiple, complementary formats, such as:

- clear visual signage in reception or common areas;
- verbal explanations or staff-assisted communication;
- audio announcements where appropriate;
- written messages in simple and clear language.

For example, if digital displays or mobile notifications are unavailable, physical signage or direct staff communication may become the primary method of informing

guests. Ensuring accessibility in crisis situations is not only a matter of service quality, but also of safety, inclusion, and legal responsibility.

Communication and Legal Compliance

In incidents potentially involving personal data, communication intersects directly with regulatory obligations. Under the GDPR framework (GDPR Articles 33 and 34), **notification to supervisory authorities** and, where required, **affected individuals** must follow structured assessment rather than emotional reaction. Public messaging should therefore be aligned with legal advice to ensure compliance while preserving investigative integrity.

Transparent communication demonstrates accountability; however, premature disclosure may compromise forensic evidence or escalate liability. The balance between transparency and control is a central leadership responsibility during crisis management.

Practical Activity – Communication Simulation

Objective: Draft structured internal and external communication during a digital incident.

Format: Small group drafting task

Estimated Duration: 45 minutes

Learners work in small groups to draft three short communication outputs based on a simulated incident:

1. A short internal briefing (max. 150 words).
2. A guest-facing holding statement.
3. A response to a media enquiry.

Each group must justify what information was included, what was intentionally withheld, and how regulatory considerations influenced wording choices. The emphasis is not only on content, but on reasoning and proportionality.

Going beyond: Crisis Communication as a Structured Cycle

Advanced crisis management recognises that communication evolves through distinct phases rather than occurring as a single reaction. In digital incidents, communication typically follows four stages: **preparation, immediate response, stabilisation, and trust rebuilding**.

Preparation involves predefined roles, templates, and escalation pathways. Immediate response focuses on internal alignment and controlled external messaging. Stabilisation requires consistent updates and regulatory coordination. Trust rebuilding extends beyond technical recovery and emphasises visible corrective measures and long-term reassurance.

Understanding communication as a cycle helps organisations avoid reactive messaging and maintain strategic control during digital crises.

Reflection & Discussion

01

What should be the first internal communication step when an incident is detected, and why?

02

Why must guest communication avoid speculation and maintain consistency?

6. Post-Incident Recovery & Trust

After a digital incident, recovery must be both **rapid** and **structured**. Early decisions determine whether disruption is contained efficiently or evolves into prolonged instability. The initial priority is technical stabilisation: **isolating affected systems, restoring verified clean backups, and securing access points to prevent recurrence.**

However, recovery extends beyond technical repair. Recovery governance must follow the structured response principles outlined in previous sections. Fragmented or undocumented corrective actions weaken long-term resilience and may expose the organisation to secondary regulatory review. **Effective recovery** therefore combines technical restoration with disciplined documentation, regulatory assessment, and transparent communication.

Core recovery measures include:

- verifying backup integrity before restoration;
- applying short-term compensating controls to reduce residual risk;
- conducting targeted forensic review to confirm scope and impact;
- documenting all actions for compliance and audit purposes.

Once systems are stabilised, attention shifts toward rebuilding confidence. This requires consistent and credible actions rather than reassurance alone. Organisations should **communicate corrective measures clearly**, demonstrate security improvements such as strengthened access controls or segmentation, and **provide accessible contact channels for affected stakeholders**.

Staff support is also critical during recovery. Fatigue and operational pressure increase the likelihood of secondary errors. Structured schedules, clear task allocation, and post-incident training reinforce resilience and demonstrate organisational responsibility.

Sustainable recovery integrates technical remediation, governance reinforcement, and trust rebuilding. When managed properly, the recovery phase becomes an opportunity to strengthen long-term resilience rather than merely restore previous conditions.

Going Beyond

Advanced recovery planning extends beyond immediate stabilisation. Long-term trust rebuilding may include independent verification measures such as third-party audits or certifications, structured transparency updates to customers and partners, strengthened supplier assurance mechanisms, and investment in continuous monitoring and resilient backup architecture (including immutable backups).

Such measures ensure that recovery is not reactive but transformative. Strategic post-incident investment should be proportional to organisational size and exposure, balancing cost with measurable reductions in future risk and reputational vulnerability.

Reflection & Discussion

01

Identify three immediate priorities during the recovery phase. Explain why these actions must be addressed before long-term improvements begin.

02

Why is structured documentation of recovery actions essential? Consider its role in regulatory compliance, internal learning, accountability, and stakeholder trust.

03

Which long-term measures most effectively rebuild digital trust in a tourism organisation? Evaluate whether technical upgrades, transparency measures, independent audits, supplier assurance, or staff training have the greatest long-term impact, and justify your reasoning.

Concluding Perspective: Digital Security as Governance

Digital security in tourism should not be understood as a purely technical function but as an integrated governance discipline combining operational vigilance, regulatory awareness, structured risk prioritisation, and coordinated crisis management. Sustainable resilience emerges from disciplined daily practices supported by proportional technological controls.

7. Final Discussion & Evaluation

Exercise – Reflective Consolidation Discussion

Objective: Consolidate conceptual understanding and encourage self-assessment of professional accountability in digital security environments.

Format: Group reflection

Estimated Duration: 20–30 minutes

Participants discuss the following reflection points and connect them to real tourism operational contexts:

- How would you recognise that a technical or data-related issue is becoming a digital incident?
- At what point should an issue be escalated instead of handled individually?

Training Unit 2: Digital Security in Tourism

- How do procedures and documentation help during high-pressure situations?
- What communication behaviours help protect customer trust during and after incidents?
- How does your own behaviour influence colleagues, customers, and recovery outcomes?

Final Evaluation Quiz

Objective: Assess theoretical understanding and applied decision-making competence across all components of Unit 2.

Format: Individual assessment

Estimated Duration: 25–35 minutes

Questions:

1. When a digital incident is suspected, which action should occur first?

- A. Attempt to resolve the issue independently before informing others
- B. Wait until full technical confirmation is available
- C. Escalate through the defined reporting channel immediately
- D. Inform guests before internal teams are notified

Correct answer: C

2. Which course concept most directly reinforces personal responsibility in digital security?

- A. Advanced encryption standards
- B. Zero Trust principles and early escalation discipline
- C. Blockchain verification mechanisms
- D. Media communication templates

Correct answer: B

3. Why does structured communication reduce the impact of digital incidents?

- A. It eliminates the need for technical containment
- B. It prevents confusion, duplication of actions, and reputational escalation
- C. It replaces regulatory notification requirements
- D. It ensures incidents remain confidential

Correct answer: B

4. Which behaviour most significantly reduces digital risk in everyday operations?

- A. Sharing credentials only with trusted colleagues
- B. Ignoring minor anomalies during busy periods
- C. Reporting suspicious activity early and following procedures
- D. Relying solely on IT to detect threats

Correct answer: C

5. At what point should an operational issue be escalated as a potential digital incident?

- A. Only after customers complain
- B. When there is reasonable suspicion of data compromise or system misuse
- C. After management approval is requested
- D. When the media becomes involved

Correct answer: B

6. Which practice most effectively strengthens long-term digital resilience?

- A. Restoring systems quickly without documentation
- B. Conducting root cause analysis and implementing structural improvements
- C. Minimising communication to avoid reputational damage

D. Treating incidents as isolated technical failures

Correct answer: B

7. Which communication behaviour protects customer trust during a crisis?

- A. Providing detailed technical explanations immediately
- B. Speculating about possible causes to appear transparent
- C. Delivering verified, consistent, and empathetic updates
- D. Avoiding public statements until the investigation is fully completed

Correct answer: C

8. Which combination best reflects a disciplined recovery approach?

- A. Rapid system restart, minimal documentation, delayed communication
- B. Technical containment, documented actions, regulatory assessment, coordinated messaging
- C. Public apology before confirming impact
- D. Isolating IT from management decision-making

Correct answer: B

9. Which TWO factors most commonly allow a minor issue to escalate into a digital crisis?

- A. Delayed escalation due to uncertainty
- B. Immediate transparent communication to regulators
- C. Procedural shortcuts under operational pressure
- D. Strong network segmentation

Correct answers: A and C

10. Which TWO elements are essential for effective regulatory compliance during an incident involving personal data?

- A. Immediate public press release
- B. Structured documentation of actions taken
- C. Risk assessment of impact on individuals
- D. Internal deletion of suspicious logs

Correct answers: B and C

11. Which TWO measures most effectively reduce the likelihood of ransomware spreading across systems?

- A. Network segmentation
- B. Sharing administrator credentials only within management
- C. Offline or immutable backups
- D. Avoiding communication with external forensic specialists

Correct answers: A and C

12. Which TWO communication practices strengthen organisational credibility during a crisis?

- A. A single authorised spokesperson
- B. Multiple departments responding independently
- C. Consistent messaging across channels
- D. Immediate disclosure of unverified technical details

Correct answers: A and C

13. Which TWO behaviours demonstrate strong professional accountability in digital tourism environments?

- A. Reporting anomalies even if uncertain
- B. Attempting to resolve suspected breaches independently
- C. Following defined escalation procedures

D. Waiting for direct managerial instruction before acting

Correct answers: A and C

3

REFERENCES

1. European Commission. (2024). *The EU Pact for Skills – Skills Partnership for the Tourism Ecosystem (Baseline update)*. <https://pact-for-skills.ec.europa.eu/>
2. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2). (2015). *Official Journal of the European Union*, L 337. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). (2019). *Official Journal of the European Union*, L 151. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). (2022). *Official Journal of the European Union*, L 333. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
6. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). (2022). *Official Journal of the European Union*, L 152. <https://eur-lex.europa.eu/eli/reg/2022/868/oj>
7. European Union Agency for Cybersecurity (ENISA). (2022). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

8. European Union Agency for Cybersecurity (ENISA). (2025). *Technical implementation guidance on cybersecurity risk management measures (Version 1.0)*. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
9. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. <https://www.iso.org/standard/27001>
10. World Tourism Organization (UNWTO). (n.d.). *Global code of ethics for tourism*. <https://www.untourism.int/global-code-of-ethics-for-tourism>



 treadsproject.eu

 [treads-project](https://www.linkedin.com/company/treads-project)

 [Treads Project](https://www.facebook.com/TreadsProject)

 [treadsprojecteu](https://www.instagram.com/treadsprojecteu)



Co-funded by the
European Union

Co-funded by the European Union. The opinions and views 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