MODULE 6 – ONLINE PAYMENTS

UNIT 6.2
Best practices and online payments safety

LESSON INTRO	With the rise of online shopping and digital transactions, it's vital to keep your online payments safe to protect your financial information. Online payment safety involves steps to safeguard your personal and financial details when making purchases or transactions online. By understanding the risks and taking precautions, you can reduce the chances of fraud or identity theft. Online payment safety involves measures to safeguard your personal and financial details from falling into the wrong hands. One essential aspect is being phishing aware. In this lesson, you will learn how to be safe when performing online payments thanks to a list of best practices and tips about online safety when financial aspects are present.
PREVIOUS ASSIGNMENT(s) CHECK	During the role-playing exercise, seniors will take on different roles, according to the research they have conducted in the assignment execution. Leave room for free expression and rich interaction among learners, intervene only when necessary. This approach enables them to explore real-life situations and develop practical skills for navigating online payments safely.
INTRODUCTION TO THE TOPIC	The best method for online payment safety is to keep your software updated regularly. This includes your operating system, web browser, and any security software you use. Updates often include fixes for known security issues,

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	which helps protect your personal and financial information from cyber threats. Enable automatic updates whenever possible to ensure you're using the most secure software versions. Using secure websites is crucial when making online transactions. Look for "https" in the URL, indicating a secure connection that encrypts your data. Avoid entering sensitive information on websites without this secure connection, and be cautious of sites asking for unnecessary personal details. It's better to be cautious when in doubt about a website's legitimacy. Monitoring your account activity is essential for online payment safety. Regularly check your account statements and transaction history to spot any unauthorized or suspicious activity. Review your account at least weekly, and set up alerts for large or unusual transactions to stay informed in real-time. If you notice any unauthorized or suspicious transactions, report them to your financial institution immediately. Most banks and credit card companies have fraud departments to investigate and resolve such issues. Keeping records of your communications with your financial institution about suspicious transactions is advisable for future reference. Additionally, take proactive steps to protect your online payment information. Use secure and unique passwords for your accounts, enable two-factor authentication, and avoid using public Wi-Fi networks for online payments.
GENERAL THEORY	Regarding security, online payment systems have advanced measures to protect sensitive information. Encryption technology secures data transmissions, and two-factor authentication verifies users' identities, minimizing fraud risks. Despite these

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	safeguards, users should still take precautions like using strong passwords, avoiding public Wi-Fi for transactions, and monitoring accounts regularly to prevent cyber threats. Online payments offer several benefits to consumers, including convenience, flexibility, and security. Making payments online is convenient as customers can do it anytime and anywhere with an internet connection, eliminating the need to visit a physical store or bank. Additionally, online payments provide flexibility by offering various payment options like credit cards, debit cards, and digital wallets. Phishing scams often involve fraudulent emails or messages that impersonate trusted entities to trick you into revealing sensitive information. To avoid falling victim, be cautious of unsolicited emails, and never click on suspicious links or provide personal information. Best practices on online payment safety can be: 1) Use a Virtual Private Network (VPN): Consider using a VPN when making online payments, especially when using public Wi-Fi networks. A VPN encrypts your internet connection, providing an added layer of security and privacy. 2) Regularly review privacy settings: Take the time to review and update the privacy settings on your accounts and devices regularly. Limit the amount of personal information shared online to minimize the risk of identity theft and unauthorized access to your accounts. 3) Be cautious of email and phone scams: Be wary of unsolicited emails or phone calls requesting personal or financial information, even if they appear to be from legitimate sources. Avoid clicking

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	on links or downloading attachments from unknown or suspicious sources. 4) Enable multi-factor authentication: Whenever possible, enable multi-factor authentication (MFA) for your online accounts. MFA adds an extra layer of security by requiring additional verification beyond just a password, such as a one-time code sent to your phone. **5)** Keep backups of important data: Regularly back up important documents and data stored on your devices, such as financial records and transaction receipts. In the event of a security breach or data loss, having backups ensures you can still access crucial information.
REGIONAL THEORY	We have summarized and translated a recent study from 'Il Sole 24 Ore' (https://www.ilsole24ore.com/art/la-sicurezza-informatica-passa-nuovi-modelli-relazione-i-cittadini-clienti-AF3AldXC) providing for some very interesting data on the latest development at Italian level on the topic of online payments: In Europe and in Italy, there is an urgent need to quickly and effectively bridge the gap in cybersecurity defenses for both the country's system and individual strategic assets, starting with small and large businesses. Both Central Public Administration (CPA) and Local Public Administration (LPA) handle sensitive information daily and provide critical and often indispensable services. This shift towards strengthening cybersecurity is supported by recent regulations, both at the European (EU Regulation 7 Jan. 2023/2841) and national levels (Draft Law on Cybersecurity approved by the Council of Ministers on January 25). These regulations aim to accelerate and promote the adoption of concrete measures to mitigate the cyber risk faced by both public and private entities.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	In recent years, cyberattacks have grown in number and effectiveness, impacting the operations of companies and public administrations that provide strategic services and manage sensitive data. The economic consequences and elevated service disruptions affect communities, citizens-users, and customers. Key institutions cannot be left exposed to such risks, especially considering the political, economic, and social instability resulting from international conflict scenarios. The issuance of the new European Regulation aims to expedite the country's adaptation and response to cyber risks by establishing measures to increase cybersecurity levels within EU institutions and bodies. The regulation defines measures for establishing an internal framework for risk management, governance, and control for each entity, and establishes a new Interinstitutional Committee for Cybersecurity (IICB) tasked with monitoring and supporting the correct implementation of the new rules. At the national level, the draft law on Cybersecurity expands the range of subjects required to report a relevant incident. It mandates entities to develop an internal structure responsible for defining strategies for managing cybersecurity risks and implementing action plans and risk monitoring. The draft law also introduces a new hypothesis of state liability and administrative sanctions in cases of non-compliance with the established obligations. There is undoubtedly increased sensitivity to these issues within the cybersecurity market. Public and private organizations are beginning to approach digital transformation with a focus on "secure digital innovation," emphasizing attention to cybersecurity aspects through advanced tools to detect breaches, define more effective response strategies, and

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	provide innovative defense services for strategic assets. The benefits are objectively significant because reputational costs, service interruptions, and information loss are real, and no prudent public official can ignore them or refrain from taking action to counter them. This transformation entails a complete rethink of operational processes in a perspective of profound innovation, enabled by new models of user relations and service delivery. Innovation brings about positive transformation not only for the institution itself but also for citizens and private individuals who benefit from the services. It is the responsibility of industry operators to make access to advanced cybersecurity services more "democratic." The challenge is to make these services increasingly simple, easy to configure and manage, and accessible to small and medium organizations without sacrificing effectiveness.
EXAMPLES (BOTH REGIONAL AND NON-SPECIFIC)	1. Maria, a senior citizen, regularly shops online for groceries. Before making any purchases, she always checks for the padlock symbol in the browser's address bar and ensures that the website's URL starts with "https://" to confirm that the website is secure. By following this practice, Mary protects her personal and financial information from potential cyber threats. 2.Giovanni, another senior, frequently checks his bank account statements and credit card transactions online. Recently, he noticed a suspicious transaction on his credit card statement. Without delay, John reported the unauthorized charge to his bank, which promptly investigated the issue and refunded the amount. John's vigilance in monitoring his account activity helped him detect and address potential fraudulent activity swiftly.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	3. Sara, a retired professional, enjoys using various online services for communication and entertainment. To ensure the security of her accounts, Sarah follows the advice of creating strong and unique passwords for each of her online accounts. She uses a combination of letters, numbers, and special characters and avoids using easily guessable information like her name or birthdate. By maintaining strong passwords, Sarah reduces the risk of unauthorized access to her online accounts.
HANDS ON EXPERIENCE	What is one of the best practices for ensuring online payment safety? a. Sharing passwords with friends b. Using public Wi-Fi for transactions c. Checking for the padlock symbol in the browser's address bar d. Clicking on suspicious links in emails Which of the following is a secure payment method for online transactions? a. Sending cash in an envelope b. Using a credit card with encryption technology c. Providing your social security number to unknown websites d. Sharing your PIN number with online retailers How often should you monitor your financial statements and credit reports for suspicious activity? a. Never b. Once a year c. At least once a month d. Only when you receive a notification from your bank What should you do if you notice unauthorized transactions on your account? a. Ignore them, as they will likely resolve on their own b. Report them to your financial institution immediately

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	c. Wait for the next statement to see if they happen again d. Share the information on social media to warn others Which of the following is NOT a recommended practice for online payment safety? a. Using strong and unique passwords for each online account b. Avoiding public Wi-Fi networks for transactions c. Clicking on links in emails from unknown senders d. Checking for secure connections on websites before entering sensitive information *Correct answers* *1 – C* *2 – B* *3 – C* *4 – B* *5 - C*
DISCUSSION	In an era of increasing digitization, do you believe that traditional payment methods, like cash or checks, still hold relevance, or are they becoming obsolete in favor of online payments? Why? "How can we strike a balance between embracing the convenience of online payments while also ensuring the security of our financial information? What measures do you think are necessary to achieve this balance?
FEEDBACK AND ASSIGNMENT	The objective of this assignment is to empower seniors with the knowledge and skills to enhance their online payment security through the development and implementation of a personalized Online Payment Security Checklist. In this assignment, seniors will develop a comprehensive Online Payment Security Checklist, focusing on essential security measures for online transactions such as

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393

	website security, password management, and safe payment methods. They will then review their current online payment practices, including the websites they use, payment methods employed, and password management strategies. After comparing their practices with the checklist items, they will identify any gaps or areas for improvement in their online payment security. Based on this evaluation, seniors will make necessary adjustments to their practices, implementing additional security measures or changing existing ones to enhance security. Finally, they will write a brief reflection discussing any challenges encountered during the assessment and adjustment phase and reflecting on the importance of online payment security for personal financial safety.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only for the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Key Action 2 – Small-scale Partnerships in Adult Education
Project Number: 2022-2-EL01-KA210-ADU-000093393