13+

Securing Personal Information on Digital Platforms (Security Settings)

SUBJECT: Safe Online Navigation

LESSON TOPIC: Security Settings

DURATION: 45 minutes (1 Lesson); 1-1.5 hours (Preparation)

LEARNING OBJECTIVES:

Main Objective: Students will learn how to secure sensitive personal information on digital platforms, including ID information, credit card data, health information, home address, phone numbers, and other personal identifiers beyond just using strong passwords.

Competencies Acquired:

- Students will understand the importance of protecting various types of personal information online.
- They will learn best practices for securing sensitive data such as ID information, credit card details, health records, home addresses, and phone numbers.
- They will become aware of the potential risks associated with inadequate protection of personal information and how to mitigate these risks.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

MATERIALS/RESOURCES NEEDED:

- Module 2 (https://www.digi-civis.eu/e-learning)
- A device with internet access (if available) for demonstrating security settings related to personal information.
- Pre-prepared scenarios and examples (provided below) to discuss during the lesson.
- Quiz questions (provided below).

METHODS/TECHNIQUES:

- **Presentation:** The teacher delivers a concise and engaging overview of key topics, emphasizing the importance of securing various types of personal information online.
- **Group Work (Case Scenario Analysis)**: Students are divided into small groups to discuss and solve specific scenarios related to the protection of personal information.
- **Quiz:** A short quiz is administered to assess students' understanding of the key concepts discussed during the lesson. This helps to reinforce learning and identify any areas that may need further clarification.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

LESSON PLAN OVERVIEW

PREPARATION:

The teacher must:

- Thoroughly go through Module 2 that cover the fundamentals of security settings on digital platforms.
- Familiarize yourself with the specific security settings related to personal information, such as ID protection, credit card security, and safeguarding health information, home addresses, and phone numbers.
- Print, and cut out scenarios for the group work activity.
- Print the quiz questions that will be used to assess students' understanding at the end of the lesson.

IMPLEMENTATION:

1. Introduction/Short Presentation (15 minutes):

Overview of the Topic: Explain the essential concepts related to ID information, credit card details, birthdates, health records, and home addresses.

Explanation: ID information includes personal identifiers such as Social Security numbers (SSNs), driver's license numbers, and passport numbers. These pieces of information are critical for verifying a person's identity and can be used to commit identity theft if they fall into the wrong hands. Identity theft occurs when someone illegally uses another person's personal information to gain financial benefits or other advantages.

Why it's important: ID information is a primary target for cybercriminals because it can be used to open bank accounts, apply for loans, or commit fraud.

Best practices:

- Never share your SSN, driver's license number, or passport number unless absolutely necessary.
- Store physical copies of these documents in a secure place (e.g., a locked drawer or safe).
- When providing ID information online, ensure the website is secure (look for "https" and a padlock icon).

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

- Monitor your credit report regularly to catch any unauthorized use of your ID information.

Explanation: Credit card data includes your card number, expiration date, CVV (Card Verification Value), and billing address. This information is sensitive because it allows others to make purchases or withdraw money from your account.

Why it's important: Credit card fraud is a common form of financial crime where thieves use stolen card information to make unauthorized purchases.

Best practices:

- Only enter your credit card information on secure, trusted websites.
- Use virtual credit card numbers or digital wallets (e.g., Apple Pay, Google Pay) for online transactions.
- Set up alerts with your bank or credit card company to be notified of any unusual activity.
- Regularly review your bank statements for unauthorized transactions.

Explanation: Personal identifiers like birthdates, email addresses, and even usernames can be used by criminals to guess passwords, answer security questions, or build a profile for identity theft.

Why it's important: Birthdates are often used in combination with other data to reset passwords or verify identities.

Best practices:

- Be cautious about sharing your full birthdate online; consider only sharing the month and day if needed.
- Use different email addresses for different types of accounts (e.g., one for banking, another for social media).
- Avoid using the same username across multiple platforms to make it harder for someone to link your accounts.
- Be mindful of how much personal information you share on social media profiles.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

Explanation: Health information includes medical records, insurance details, and any data related to a person's physical or mental health. With the rise of online health services and electronic medical records, protecting this information has become increasingly important.

Why it's important: Health information is highly sensitive and can be used for identity theft, insurance fraud, or even blackmail if disclosed improperly.

Best practices:

- Use secure, encrypted communication channels when sharing health information online.
- Verify the security of online health portals before entering any personal health details.
- Be cautious of sharing health information on social media or in public forums.
- Enable two-factor authentication on health portals whenever possible.

Explanation: A home address is a personal piece of information that can reveal where you live. If exposed online, it can lead to various risks, including stalking, burglary, and scams.

Why it's important: Knowing someone's home address can allow criminals to target them physically (e.g., for theft) or use the information to scam them (e.g., fake delivery scams).

Best practices:

- Avoid sharing your home address publicly online, such as on social media or public forums.
- Use a P.O. box for deliveries if you frequently shop online or sell items.
- Ensure any platforms that require your home address (e.g., online marketplaces) have robust privacy settings.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

- Be cautious of unsolicited requests for your address, especially over the phone or through email.

Explanation: Phone numbers are often used for verification and contact purposes. However, they can also be exploited for scams, identity theft, or unwanted marketing if not properly protected.

Why it's important: Phone numbers can be used in SIM-swapping attacks, where a hacker takes control of your phone number to access your online accounts.

Best practices:

- Avoid sharing your phone number publicly online, especially on social media.
- Use two-factor authentication apps instead of SMS where possible to reduce the risk of SIM-swapping.
- Consider using a secondary phone number or an app-based number for non-essential services.
- Be cautious of unsolicited calls or texts asking for personal information.

2. Case Scenario Group Work (20 minutes):

Scenario 1: A student receives a text message claiming to be from their bank, asking them to verify their home address and phone number. What should they do?

Expected solutions (For the teacher: Do not share this with students)

1. Do not respond to the text message.
2. Contact the bank directly using a known phone number to verify if the request is legitimate.
3. Report the suspicious message to the bank's fraud department.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

Scenario 2: A user frequently shares their location and pictures of their home on social media. Discuss the risks involved and what steps they should take to protect their privacy.

Expected solutions (For the teacher: Do not share this with students)

1. Avoid sharing specific location details in real-time.
2. Adjust privacy settings to limit who can view posts.
3. Be cautious about tagging locations or mentioning home details in posts.

Scenario 3: Someone receives an unsolicited phone call from someone claiming to be from their healthcare provider, asking for their health insurance number and other personal details. How should they respond?

Expected solutions (For the teacher: Do not share this with students)

1. Do not provide any information over the phone.
2. Hang up and contact the healthcare provider directly using a verified phone number.
3. Report the call to the healthcare provider's fraud department.

Scenario 4: A person lists their home address and phone number on an online marketplace profile to make selling items more convenient. Discuss the potential risks and how to mitigate them.

Expected solutions (For the teacher: Do not share this with students)

1. Use the platform's private messaging system instead of sharing personal contact information.
2. Consider using a P.O. box or a temporary phone number.
3. Meet buyers in public places rather than giving out a home address.

Each group (3-5 students) discusses their assigned scenario and presents their proposed solutions to the class, explaining the rationale behind each step.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

ADDITIONAL INFORMATION TO LEARN MORE:

- 11 Internet Safety Tips for Your Online Security https://www.youtube.com/watch?v=aO858HyFbKI&t=21s
- Online Privacy & Security 101: How To Actually Protect Yourself? https://www.youtube.com/watch?v=qZE45J-MIUg

ANNEXES:

- Assessment Quiz

HOMEWORK:

Task: Students should review and secure the personal information they share online, including home address, phone number, birthdate, and other personal details. They should apply at least one new security measure discussed in class.

Reflection: Write a brief paragraph about the changes they made and how they believe these changes will better protect their personal information.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.

ASSESSMENT:

- Assess students based on their involvement in group discussions and the quality of solutions they present.
- Grade the quiz responses to ensure understanding of the key concepts.
- Encourage students to share one new action they plan to take to secure their personal information online, explaining why it is necessary.

Quiz (15 minutes):

Written Quiz:

1. Question: Why is it important not to share your home address publicly online?

(Answer: Sharing your home address publicly can make you a target for burglary, scams, and unwanted visitors.)

2. Question: What should you do if you receive a suspicious call asking for your personal information?

(Answer: Do not provide any information; hang up and contact the organization directly using a verified contact method.)

3. Question: How can sharing your phone number online put you at risk?

(Answer: Your phone number can be used for identity theft, SIM-swapping attacks, and unwanted marketing.)

4. Question: What are the risks of sharing your health information over unsecured channels?

(Answer: Health information can be intercepted, leading to privacy breaches or identity theft.)

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union can be held responsible for them.