Training Fiche E-Seniors

|  |  |
| --- | --- |
| **Title** | **Topic: Information and communication through social media**  **Unit 3. Threats and challenges on social media: DOs and DONTs** |
| **Training Area** | *Please select one or more of the following:*   |  |  | | --- | --- | | Online Security |  | | Cultural and Media Literacy | *X* | | Economic Transactions |  | | Personal Data Protection |  | | Digital Identity and online reputation |  | |
| **Keywords (meta tag)** | **Social media, communication, safety** |
| **Provided by** | **E-Seniors** |
| **Language** | **English** |
| **Objectives / goals / learning outcomes** | |
| This module aims to develop the knowledge and skills of the users on how to use social media for communication and the promotion of culture and creativity. Senior users will get familiar with the social media tools, cultural resources on social media that enable them to easily navigate and discover cultural and communication opportunities. | |
| **Description** | |
| The course is arranged into 3 levels: each module is divided into units and contents. The titles of the units give a more detailed idea about the content of the module. This specific module is built as follows:  **Topic: Information and communication through social media**  **Module 3. Threats and challenges on social media: DOs and DONTs**  **Unit 3.1:** Threats and challenges  **Unit 3.2:** 10 good practices to adopt for security on social networks. | |
| **Contents arranged in 3 levels** | |
| **Module 3: Threats and challenges on social media: DOs and DONTs**  There are many threats and challenges involved in browsing the internet, both on the computer and the smartphone. Social networks are not an exception. There are several risks involved in using social networks. However, if precautions are taken, it is not difficult to surf with minimal risk.  **Unit 3.1:** Threats and challenges   * **Phishing:** Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim. These messages are designed to trick you into revealing personal information by pretending to be from a trusted source. The messages may come from people claiming to be a friend of yours or a known company. Never share confidential information and never click on a suspicious-looking web link. * **Psychological hacking:** Psychological hacking is the process of obtaining confidential information from a person through trickery. The fraudster may start a conversation about things they read on your profile, such as where you work, etc. They then try to get you to reveal personal information, similar to phishing. * **Malware:** Malware is malicious software designed to infiltrate devices. It circulates on social networks as links with catchy titles. Once the malware is infiltrated, it can send messages to contacts, access personal information, or damage the device. Caution should be exercised when tempted to click on a link from an unknown source. * **Hate speech:** Hate speech is common on social networks because its authors can remain anonymous. It can happen that you receive hate speech, sometimes without any network, so it is important to detach yourself from it and not hesitate to report it as unwanted and malicious content. * **Cyberbullying:** is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior. * **Ageism online**: Ageism refers to the stereotypes (how we think), prejudice (how we feel) and discrimination (how we act) towards others or oneself based on age. Ageism affects everyone. Children as young as 4 years old become aware of their culture’s age stereotypes. From that age onwards they internalize and use these stereotypes to guide their feelings and behavior towards people of different ages. They also draw on culture’s age stereotypes to perceive and understand themselves, which can result in self-directed ageism at any age. Ageism intersects and exacerbates other forms of disadvantage including those related to sex, race and disability. * **What to watch out for to avoid Facebook Scams:**    + People you don't know personally asking you for money or your bank details.   + Unverified Pages claiming to represent a large organization or public figure.   + People who ask you to continue your conversation outside of Facebook, in a less public or less secure setting, such as a separate email address.   + People asking you to send them your bank details in order to receive a reward.   + Anyone claiming to be a friend or relative of yours in distress.   + People who lie about where they live.   + Posts or publications containing spelling mistakes and grammatical errors.   + People or accounts that redirect you to a Page to claim a prize   **Unit 3.2: 10 good practices to adopt for security on social networks:**  1- **Protect access to your accounts:** Use strong passwords that are different from one account to another. Password manager applications can help you to easily save your passwords. For example **https://keepassxc.org/**  2- **Check your privacy settings**: By default, the privacy settings are often open (on personal information such as name, phone number, email address). This data can be accessible to all subscribers of the social network. It is possible to limit this visibility by adjusting the account configuration to keep control of what other users see.  3- **Control your posts:** Your posts can get out of hand and be reposted or interpreted more than you intended. Do not post personal or sensitive information.  4- **Be careful who you talk to,** Your friends may be sharing malicious content without knowing it, or may have been hacked themselves. Never send money without verifying the person's identity, don't send private videos, be suspicious of contests, unexpected winnings, or "great deals" that may hide scams.  5-  **Control third-party applications:** Some applications offer to interact with one of your social network accounts. They require permissions that need to be examined carefully, as some of them may then have access to your data. Be careful not to install applications that you suspect of being malicious.  6- **Avoid public computers and networks:** Using an open-access computer or public Wi-Fi is risky as they may be compromised or under the control of cybercriminals. Avoid entering sensitive information or using them if possible.  7- **Check your account logins regularly:** Most social networks allow you to see active account connections or sessions. Check this information regularly to make sure that another device is not connected to one of your accounts. If it is, disconnect it and change your password.  8- **Be aware of fake news:** Some published information may be false, deliberately, or not. Before considering or relaying any information, check its authenticity.  9- **Check your identifications with your accounts:** Some websites offer to register you with your social network account. This avoids the need to create a password, for example, but may provide personal data to the site or allow a cybercriminal who has hacked your social network to access your account on that site as well.  10- **Delete your account if you no longer use it:** To avoid all the risks described above, to ensure that your account is not used without your knowledge, delete your account when you no longer need it. | |
| **Contents in bullet points** | |
| * The most frequent threats and challenges of using social media is to defend yourself from phishing, malware, hate speech, etc.; * You can avoid social media threats and risks by following recommendations and advice stipulated in this training module | |
| **5 glossary entries** | |
| **Social media safety:** Social media security refers to all the measures that the user should take to avoid risks, scams, and attacks on their personal account.  **Hate speech:** Hate speech is spoken words that are offensive, insulting, and/or threatening to an individual or group based on a particular attribute of that person or persons being targeted.  **Psychological hacking:** Psychological hacking is the process of obtaining confidential information from a person through trickery.  **Cyberbullying:** is bullying that takes place over digital devices like cell phones, computers, and tablets  **Ageism online**: Ageism refers to the stereotypes (how we think), prejudice (how we feel) and discrimination (how we act) towards others or oneself based on age. Ageism affects everyone. | |
| **Bibliography and Further References** | |
| [**https://understandthesocialmedia.com/**](https://understandthesocialmedia.com/)  [**https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf**](https://wtccentralpa.org/wp-content/uploads/2013/01/socialmedia-2.pdf) | |
| **Five multiple-choice self-assessment questions** | **1) It is safe to use public computers**   1. **True** 2. **False**   **Correct: B**  **2) What is Malware?**   1. **Malicious software designed to infiltrate devices** 2. **Identity fraud** 3. **Hate speech**   **Correct: A**  **3) What is hate speech?**   1. **Hate speech is spoken words that are offensive, insulting, and/or threatening to an individual or group based on a particular attribute of that person or persons being targeted.** 2. **Hate speech is the process of obtaining confidential information from a person through trickery.** 3. **Hate speech is malicious information designed to infiltrate devices and attack humans.**   **Correct: A**  **4) Social media safety:**   1. **Refers all the measures that companies use to defend online fraud.** 2. **Refers to all the measures that the user should take to avoid risks, scams, and attacks on their personal account.** 3. **Refer tools the social media designed for the users.**   **Correct: B**  **5) What to do if you come across the online hate speech?**   1. **Try to avoid the attackers** 2. **Try to report the attackers** 3. **All of the above are correct**   **Correct: C** |
| **Related Material** | **How to Identify and Avoid Common Social Media Scams:** [**https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/**](https://www.onpointcu.com/blog/how-to-identify-and-avoid-common-social-media-scams/)  **How to avoid social media fraud:** [**https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html**](https://www.nbc.ca/personal/advice/security/social-medias-fraud-scams.html)  **Cyberbullying and Hate Speech:** [**https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf**](https://www.ditchthelabel.org/wp-content/uploads/2020/05/Cyberbullying-and-hate-speech.pdf) |
| **Related PPT** |  |
| **Reference Link** | **https://www.stopbullying.gov/cyberbullying/what-is-it** |
| **Video in YouTube format (if any)** | **What is Social Media? In Simple English:**  [**https://www.youtube.com/watch?v=jQ8J3IHhn8A**](https://www.youtube.com/watch?v=jQ8J3IHhn8A)  **Amazing mind reader reveals his 'gift':** [**https://www.youtube.com/watch?v=F7pYHN9iC9I**](https://www.youtube.com/watch?v=F7pYHN9iC9I) |