Training Fiche CDI

|  |  |
| --- | --- |
| **Title** | How to identify missing information and fake news online in a culture relevant context |
| **Training Area** | *Please select one or more of the following:*   |  |  | | --- | --- | | Online Security | X | | Cultural and Media Literacy |  | | Economic Transactions |  | | Personal Data Protection |  | | Digital Identity and online reputation |  | |
| **Keywords (meta tag)** | online security, online safety, cultural context, fake news, missing information |
| **Provided by** | Community Development Institute, CDI |
| **Language** | English |
| **Objectives / goals / learning outcomes** | |
| By the end of this module you will acquire knowledge in regard to recognition of fake news and missing information as well online security in cultural context.  The module consists of four units providing information related to the topic in different sections. Different activities and acknowledgments are supported with examples for a better understanding of the material, explanatory photos and useful links to expand your knowledge on the topic.  The users will have the opportunity to be introduced with online security in a cultural context as well as online safety. The possible online security threats will be presented through explanations of the different types of threat like malware, phishing, password attacks etc.  The users will be able to:  ● Understand the meaning of online security and safety  ● Make a difference between fake news, misinformation and missing information  ● Use different tips in regard to online security in cultural context | |
| **Description** | |
| Digital technologies have revolutionized every aspect of our lives. They have impacted on the value chains of all the cultural and creative industries not only as regards the creative process and its execution but also as regards the making of a work or product of art and its promotion, distribution, marketing and sale.  This learning unit will teach late digitals to detect potential scams fraud they could meet on the web while using or searching for cultural resources. This unit will provide specific examples of common scams linked to cultural resources, like fake ticket sales, phishing attempts after ordering online etc. It will also give the key points in identifying secure cultural resources online.  In today's era of technological, fake news and missing information are part of everyday circulation and information online. The users will be introduced with what is the meaning of fake news and missing information, how to recognize fake news and the importance for differentiating between fake news and missing information.  Fostering the ability to recognise and protect yourself from missing information and fake news is the unit providing information and content in regard to ability of the users to protect themselves online. Tips and tricks are provided along with useful examples and photos. | |

|  |  |
| --- | --- |
| **Contents arranged in 3 levels** | |
| 1. **INTRODUCTION** 2. **CONTENT**   **Unit 1: What is Online Security?**  1.1 Online Security and online safety, meaning  1.2 Online security in cultural content  **Unit 2: Biggest threats to your online security**  2.1 Types of Online Security Threats   * Malware * Man in the Middle MITM * Phishing * Password Attacks   **Unit 3: Identifying missing information, misinformation, disinformation and fake news in cultural context**  3.1 Where Does Fake News Come From?  3.2 How to recognise fake news, misinformation, disinformation and missing information in cultural context  **Unit 4: Protecting yourself from online security threats**  4.1 Protect yourself while online  4.2 Tips for online security in a cultural context   1. **CONCLUSION**   **Module: How to identify missing information and fake news online in a culture relevant context**   1. **INTRODUCTION**   Digital technologies have revolutionized every aspect of our lives. They have impacted on the value chains of all the cultural and creative industries not only as regards the creative process and its execution but also as regards the making of a work or product of art and its promotion, distribution, marketing and sale. As the digital shift continues, more and more artists, filmmakers, producers, musicians and so on are distributing their products digitally. By the end of this module you will acquire knowledge and recognition of fake new and missing information as well online security in cultural context.  In a world where a hacker attack takes place roughly every 39 seconds, online security can no longer be taken lightly. Otherwise, your whole personal data could be in danger.  But what is online security, to be exact? What kind of threats are there on the web, and what can you do to protect yourself from them? An online security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Now, more than ever cultural content is widely accessible it is also open to online threats, spreading missing information, misinformation, disinformation and fake news could damage a person's experience while enjoying and informing about a cultural performance or event.  **Unit 1: What is Online Security?**  **Section 1.1 Explaining online Security and online safety**  Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.  **Online Safety** protects the people using the internet from harm through awareness, education, information and technology. Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data online, and avoiding harmful or illegal content.  **Section 1.2 Online security in cultural content**  Digital technologies have revolutionised every aspect of our lives, and culture is no exception. They have impacted on the value chains of all the cultural and creative industries not only as regards the creative process and its execution, but also as regards the making of a work or product of art and its promotion, distribution, marketing and sale. Some production processes are solely digital and technology has a huge potential to make culture accessible to all, by democratising both consumption and involvement in cultural creation.  At the same time, cultural institutions, such as museums, archives, libraries and film, television and music broadcasters have been digitising their collections in an effort to preserve them and make them more broadly available. Sometimes, digitisation is a necessary step, as in the case of analogue films, which cannot be screened in their original form anymore, as cinemas are equipped solely with digital technology.  A wealth of digital cultural content is available online either for free, for a fee, or Illegally. Such an availability and abundance of cultural content and the various ways to consult it online bring new challenges and opportunities to disrupt a person's online safety and security by various means. So it is important in this digital age to be informed and know the threats to your online security and how to protect yourself while accessing cultural content online.  **Unit 2: Biggest threats to your online security**  **Section 2.1 Types of Online Security Threats**  An online security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.  There are dozens of online security threats on the Internet, so we decided to focus on the most dangerous and common ones.  **Malware:**  Malware is malicious software such as spyware, ransomware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software that malware, once activated, can:  ● Block access to key ntwork components (ransomware)  ● Install additional harmful software  ● Covertly obtain information by transmitting data from the hard drive (spyware)  ● Disrupt individual parts, making the system inoperable    **Man in the Middle, MITM:**  A man-in-the-middle (MITM) threat occurs when malicious actors insert themselves into a two-party transaction. After interrupting the transaction, they can filter and steal data. MITM threat is realised often when a visitor uses an unsecured public Wi-Fi network. Malicious actors insert themselves between the visitor and the network, and then use malware mentioned before to install software and use data maliciously.  **Phishing:**  Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine.  **Password Attacks:**  With the right password, a malicious actor has access to a wealth of information. Social engineering is a type of password attack that is defined as “a strategy that relies heavily on human interaction and often involves tricking people into breaking standard security practices.”  Other types of password attacks include accessing a password database or outright guessing.  **Unit 3: Identifying missing information, misinformation, disinformation and fake news in cultural context**  Now, more than ever cultural content is widely accessible and open to online threats, spreading missing information, misinformation, disinformation and fake news could damage a person's experience while enjoying and informing himself about a cultural event or space.  **Section 3.1 What means fake news, misinformation and disinformation?**  **Fake news** are purposefully crafted, sensational, emotionally charged, misleading or totally fabricated information.  There are two kinds of fake news:  1. Stories that aren't true. These are entirely invented stories designed to make people believe something false, to buy a certain product, or to visit a certain website.  2. Stories that have some truth, but aren't 100 percent accurate. Again, this can be deliberate, to convince readers of a certain viewpoint, or it can be the result of an innocent mistake.  The term **misinformation** refers to information that is false or inaccurate and is often spread widely with others, regardless of an intent to deceive.  While misinformation is false information that is created and spread regardless of an intent to harm or deceive, **disinformation** is a type of misinformation that is created to be deliberately deceptive. Both forms may be shared widely, regardless of whether the sharer knows the information is wrong.  Social media platforms allow almost anyone to publish their thoughts or share stories to the world. The trouble is, most people don't check the source of the material that they view online before they share it, which can lead to fake news spreading quickly. At the same time, it's become harder to identify the original source of news stories, which can make it difficult to assess their accuracy.  **Section 3.2 How to recognise fake news, misinformation, disinformation and missing information in cultural context**  How do you spot fake news, misinformation, disinformation and missing information ask yourself the next questions and do the following :  ● **Who wrote it?** Check for the author’s name. Is the name available or is it missing? Most authors who put time into a well-researched article will likely have their name attached to it.  ● **What are their qualifications?** If the author’s name is listed, find out who the person is and what their credentials are.  ● **Check the "About Us" section**. On the top or bottom of the website, there should be a section called "About Us." This section outlines the purpose of the website.  ● **Does the article inform you of all sides of the topic?** News articles should provide you with facts from various viewpoints.  ● **Does the content match the headline of the article?** A headline should provide you with an idea of what the entire article is about, but it can also be used to persuade you to believe something before reading the article.  ● **When was this article published?** Older articles may not contain up-to-date facts and might have broken links.  ● **Was the article repurposed or updated?** Repurposed or updated content tends to have a disclaimer at the beginning or end of the article.  ● How important is the date? The date gives you an indication of when the article was published.  ● **Does this web address (URL) look correct?** Typing in the wrong web address will direct you to a webpage that you were not intending to visit. It may lead you to a page with the before mentioned online security threats.  ● **Did I find this on Social Media? Social Media platforms are not news organizations. These are platforms for people to create and/or share content.**  ● **Did I find this on a blog/website?** Blogs contain content written informally and run by an individual or small group.  **Unit 4: Protecting yourself from online security threats**  **Section 4.1 Protect yourself while online**  Here are some things you can perform better to protect yourself while online:   1. **Don’t Use Unsecured WiFi Networks**   It’s best to avoid any WiFi network that doesn’t ask you for a password, and just use your own mobile data plan instead.  **2. Use Powerful Antivirus Software**  Antivirus software is your best bet of keeping your device safe from malware infections we talked about. Don’t let the name confuse you – an antivirus program fights against viruses, but it mostly targets malware (a virus being a type of malware). Make sure you keep the program updated, and that you run frequent scans – especially after you download new files. It’s best you don’t open them up without scanning them first, in fact.  **3. Always Use a VPN Online**  A VPN (Virtual Private Network) is an online service you can use to hide your real IP address and encrypt your online communications. It’s one of the best ways to enhance your online security and hide your digital footprints. As long as the proper encryption methods are used, nobody will be able to monitor your online traffic to see what you’re doing on the Internet.  **4. Avoid Phishing Attempts**  If you receive any emails or messages claiming to be from someone close to you, your bank, or the police asking you to download shady attachments, access shortened links, or share sensitive information, ignore them. Get in touch with the alleged sender instead to find out the truth. Try googling parts of the message you received between quotes. If it’s a phishing scam, you are likely to get results of other people talking about receiving the same message.    **5. Don’t Keep Bluetooth On**  While Bluetooth has its uses, keeping it turned on at all times is quite the gamble. Back in 2017 a new Bluetooth hacking method was discovered that affected millions of devices by allowing hackers to use MITM Man in the Middle threat to obtain your device’s information.All in all, it’s better to be on the safe side and turn off Bluetooth when you’re not using it to keep your online security intact.  **6. Turn Off Location Services on Your Mobile Devices**  Location services can be really useful, but they can also be very risky, there is the fact that some applications could leak your location. If that happens, it doesn’t mean you’ll be in immediate danger. Still, your online security will be threatened.  **7. Use Script Blockers in Your Browsers**  Script blockers are browser extensions you can use to make sure the websites you access don’t run unauthorized scripts and plugins in the background that can compromise your Internet safety. Don’t forget – some scripts can be so dangerous they can take over your browser, while others can run phishing redirects or ads, or even mine for cryptocurrencies by using your CPU.  **8. Keep Your Operating System Up-to-Date**  Not installing the most recent updates on your operating system can seriously harm your online security. Because malicious actors can use potential vulnerabilities to their advantage – vulnerabilities that might have been fixed with the latest update.  **9. Consider Using Encrypted Messaging Apps and Emails**  If you want to really make sure your online communications are secure, you can try using the different apps for messaging. That feature really powerful encryption.  As for emails, it’s the same, search online for different apps and what kind of security they offer.  **10. Use Strong Passwords**  Having powerful passwords for your accounts is extremely important, but coming up with a really good one is easier said than done.  If you need some help, but here are the main ideas:  1. Use spaces if it’s allowed.  2. Only use long passwords. Ideally, don’t stick to just one word.  3. Don’t use dictionary words as your password.  4. Use both uppercase and lowercase letters, and randomly mix them up.  5. Use symbols (like $, %, or \*) in your password.  6. Include numbers in your password.  7. Try making your password a whole sentence.  8. Reverse some words you use in the password (instead of “chair” use “riahc”).  9. Also, try not to use the same password for all your accounts. It’s better to use different passwords, or at the very least variations of your main password.  **4.2 Tips for online security in a cultural context**  Thanks to the internet, there are several ways for consumers to get tickets to an upcoming event. The downside is that there are also many traps consumers need to avoid. Clicking the wrong link or trusting the wrong website could lead to a fake ticket and lost funds.  Here are some tips for how to be secure online, with a specific example of buying tickets online for a cultural event:  • **Purchase directly from the venue whenever possible**. Many official ticket sales agents now offer secondary sales options, as well. Don’t click from emails or online ads; a common ticket scam trick is to create a web address that is similar to a well-known company.  **• Consider your source**. Know the difference between a professional ticket broker (a legitimate and accredited reseller), a ticket scalper (an unregulated and unlicensed ticket seller) and a scammer selling scam tickets.  • **Know the refund policy**. You should purchase tickets only from a ticket reseller that provides clear details about the terms of the transaction. Sellers should disclose to the purchaser, prior to purchase, the location of the seats represented by the tickets, either orally or by reference to a seating chart; and, if the tickets are not available for immediate access to the purchaser, disclose when the tickets will ship or be available for pickup.  • **Use payment methods that come with protection**. Always use a credit card, so you have some recourse if the tickets are not as promised. Debit cards, wire transfer or cash transactions are risky; if the tickets are fraudulent, you most likely won’t be able to get your money back.    • **Be wary of advertisements**. When you search the web for online tickets, advertisements for cheap tickets will often appear. Use good judgment; some of these ads are going to be ticket scams, especially if the prices are low.  • **If you’re unsure, verify your tickets**. Pay a visit to the arena where the event will be held. Present your ticket to customer service and they can verify if your ticket is legitimate and show you how to tell if a ticket is fake.   1. **CONCLUSION**   Online security in a broader cultural context is a very interesting subject with cultural content being widely available it too is the subject of online threats.  Digital technologies have revolutionized every aspect of our lives. They have impacted on the value chains of all the cultural and creative industries not only as regards the creative process and its execution but also as regards the making of a work or product of art and its promotion, distribution, marketing and sale. As the digital shift continues, more and more artists, filmmakers, producers, musicians and so on are distributing their products digitally.  By the end of this module you will acquire knowledge in regards to recognition of fake new and missing information as well online security in cultural context. By using the tips and the provided examples as a guideline while online, you can foster your online security. With security threats like malware, scams, phishing, hacking, and the spreading of misinformation and disinformation fake news becoming more and more common nowadays, online security has become more important than ever.  Online Security? The Bottom Line / Key Points  Online security represents the rules you follow, actions you take, and processes that happen to ensure you are safe on the Internet. With security threats (malware, scams, phishing, hacking, etc.) becoming more and more common nowadays, online security has become more important than ever.  Usually, the best way to make sure you’re safe online is to use a strong antivirus program, a reliable VPN, powerful passwords, and script blockers (among other things).  Fake news refers to deliberate untruths, or stories that contain some truth but which aren't completely accurate, by accident or design.  Some people also claim that truthful stories are "fake news," just because they don't agree with them. This can lead to the dangerous ignoring of vital advice.  Fake news can have a negative impact on the social and cultural aspects of society, so, it's crucial to know how to separate the real from the fake news as well to recognise when there is missing information, misinformation or disinformation. You can do this by following these six steps:  1. Develop a critical mindset.  2. Check the source.  3. See who else is reporting the story.  4. Examine the evidence.  5. Don't take images at face value.  6. Check that it "sounds right." | |
| **Contents in bullet points** | |
| * Cultural content is widely accessible on internet and open to online threats, spreading missing information, misinformation, disinformation and fake news could damage a person's experience while enjoying and informing about a cultural performance or event. * Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. * An online security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. * Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data online, and avoiding harmful or illegal content. Online Safety protects the people performing actions online through awareness, education, information and technology. * There are dozens of online security threats on the Internet, this module is focused on the most dangerous and common ones, such as: Malware; Man in the Middle MITM; Phishing; Password Attacks, etc. * Internet users should know how to recognise the fake news, misinformation, disinformation and protect themselfs accordingly.Fake news can have a negative impact on the social and cultural aspects of society, so, it's crucial to know how to separate the real from the fake news as well to recognise when there is missing information, misinformation or disinformation. | |
| **5 glossary entries** | |
| **1)Online security**  Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet.  **2) Online safety**  Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data online, and avoiding harmful or illegal content. Online Safety protects the people performing actions online through awareness, education, information and technology.  **3) Cultural context**  Cultural context is related to the society where individuals are raised in and at how the culture affects behavior. It incorporates values that are learned and attitudes that are shared among groups of people. It includes beliefs, meanings, customs, ideas, language, norms.  Refers to the symbolic meaning, artistic dimension and cultural values that originate from or express cultural identities.  **4) Fake news**  False news stories, often of a sensational nature, created to be widely shared or distributed for the purpose of generating revenue, or promoting or discrediting a public figure, political movement, company, etc.  **5) Missing information**  is incomplete or inaccurate information that aims to distract from accurate information, cause confusion, or change the context of a sentence, action, activity, etc. | |
| **Bibliography and Further References** | |
| * <https://www.mindtools.com/pages/article/fake-news.htm> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.researchgate.net/publication/336951206_Fake_news_Acceptance_by_demographics_and_culture_on_social_media> * <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf> * <https://www.nature.com/articles/s41586-021-03344-2> * <https://www.kdd.org/exploration_files/8._CR.10.Misinformation_in_social_media_-_Final.pdf> * <https://academicguides.waldenu.edu/library/fakenews/examples> * <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690570/EPRS_BRI(2021)690570_EN.pdf> * <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690570> * <https://en.wikipedia.org/wiki/Fake_news> * <https://call-for-papers.sas.upenn.edu/cfp/2021/06/28/if-its-on-the-internet-it-must-be-true-the-socio-cultural-impact-of-fake-news> * <https://www.frontiersin.org/research-topics/23019/the-psychology-of-fake-news-on-social-media-who-falls-for-it-who-shares-it-why-and-can-we-help-users> * <https://researchguides.austincc.edu/c.php?g=612891&p=4258046> | |
| **Five multiple-choice self-assessment questions** | 1) An email in your inbox asks you to log in with a password for some security reason. What would you do ?   1. Nothing, I will ignore the message 2. I will do as requested, it’s a security reason 3. I will contact IT expert to have more information   **Correct answer: A**  2) You are on a website that sells free tickets for a cultural event near you. They are free of charge, and they only ask for some of your personal information. What would you do ?   1. I’ll buy the tickets and enter my personal information 2. I’ll check the website to see if its real and if it's not, then to report the site 3. I’ll share the site so that others can also get the tickets   **Correct answer: B**  3) You visited a virtual tour of a well known cultural location. You noticed missing information at one of the sites. What would you do?   1. I will fill the empty lot myself 2. I will inform the virtual tour guide for this possible error 3. I will do nothing   **Correct answer: B**  4) You are creating an account on a website, and you should create a password. Which password is the most secure?   1. Your own name 2. A random line of numbers and letters that you could write on a piece of paper to remember 3. Your social security number   **Correct answer: B**  5) Do you keep your personal information safe when using social networks   1. Yes 2. No 3. Not sure   **Correct answer: Optional, all answers are correct** |
| **Related Material** | How to identify missing information and fake news online in a culture relevant context\_PPT\_CDI |
| **Related PPT** |  |
| **Reference Link** |  |
| **Video in YouTube format (if any)** | <https://youtu.be/vPAW5j_L4-c>  <https://www.youtube.com/watch?v=0yL-k5nB65o> |