Training Fiche IWS

|  |  |
| --- | --- |
| **Title** | **Online security and creativity: what’s up?** |
| **Training Area** | *Please select one or more of the following:*   |  |  | | --- | --- | | Online Security | *X* | | Cultural and Media Literacy | *X* | | Economic Transactions |  | | Personal Data Protection |  | | Digital Identity and online reputation |  | |
| **Keywords (meta tag)** | **Scams, frauds, online security tips, Internet** |
| **Provided by** | **Internet Web Solutions** |
| **Language** | **English** |
| **Objectives / goals / learning outcomes** | |
| **At the end of this module, you will be able to be aware of online security in the digital cultural world. This unit will focus on:**  **Unit 2.1 Most common scams online: examples of the most common scams online, protecting your information online.**   * **Section 2.1.1. Introduction** * **Section 2.1.2. Job advertisement** * **Section 2.1.3. Bank scam** * **Section 2.1.4. Online shopping** * **Section 2.1.5. Third-party products** * **Section 2.1.6. Inheritance via whatsapp** * **Section 2.1.7. Scam SMS from your bank** * **Section 2.1.8. Lottery scam** * **Section 2.1.9. Fake charities**   **Unit 2.2. Online security in the cultural world, how to avoid scams specific to the cultural world (fake tickets, hacking, or phishing)**   * **Section 2.2.1 How scammers perform** * **Section 2.2.2. Steps to protect yourselfyouself** * **Unit 2.3. Online Security Tips** * **Section 2.3.1. How to set up a secure password** | |
| **Description** | |
| **This course is targeted at** **adult people, who are learning the basics** **of the Internet. The module will develop core concepts needed to assess, and protect information security systems to make late digitals aware of the potential scams or** **fraud they could meet on the web while using or searching for cultural resources. This learning unit will teach seniors how to detect the most common financial scams online and how to protect their financial information and accounts.** | |
| **Contents arranged in 3 levels** | |
| **Module 2: Online security and creativity: what’s up?**  **Unit 2.1  Most common scams online: examples of the most common scams online, protecting your information online.**  **Section 2.1.1. Introduction**  Most common scams online: examples of the most common scams online, protecting your information online.  Internet fraud is becoming more and more common due to the increasing number of people using the Internet on a daily basis.  These scams not only want your money, but they also want your information, and the latter is more difficult to detect.  The basic operation of the scams has not changed, they offer products or services in exchange for a "too good to be true" amount of money or in exchange for a few questions to obtain information.  They may also offer loans or job offers as a means of getting you to take the bait.  **Section 2.1.2. Job advertisement**  For example, a job advertisement proposes a full-time salary only with part-time daily hours and does not require any previous experience. Salary is too high, and this could be considered a first indication that the ad could be a scam.  Before filling in the form or providing information, it is always good:  - to check the authenticity of the website where the advert is published   * the quality of the images or comments in case of selling products * the company publishing the advertisement * the job allowances offered   **Section 2.1.3. Bank scam**  Other fraud attempts can impersonate an entity such as your bank or a site you frequent with the excuse that there is a great offer or something is wrong with a suspicious link.  If you think it might be important, as in the case of your bank, call them instead of clicking on the link.  **Section 2.1.4. Online shopping**  Online shopping is becoming more and more common so here are some tips for safe shopping online.  - The website must have a secure encrypted connection, the web protocol must be https. Encryption allows information to be hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or cypher. The hidden information is said to be encrypted.  - Make sure you are on a trusted website. A website that has abnormally low prices, all prices the same, no reviews, or suspicious product pictures are an indication that the website is a scam.  **Section 2.1.5. Third-party products**  Some websites sell third-party products. In these cases, you should also investigate the company from which the product comes.   * It is a good sign if the site is clear in displaying cost and shipping information, accepts several forms of payment, and sends a purchase invoice.   - If you believe the site is genuine, and you make a purchase, never save your credit card information. This will prevent someone from accessing your device and making unwanted purchases.   * Periodically check your balance and if you see any suspicious movements, report them to your bank quickly.   - If the product does not arrive, try to contact the seller or the platform where it is sold.  **Section 2.1.6. Inheritance via whatsapp**  On WhatsApp a person talks to you saying that they are very old and that they have an inheritance with no heirs, and offers you to inherit it yourself.  Another person talks to you directly about a trick to invest without risk, promising you that you can make €100,000 in just one month.  Attractive man/woman in love with you  A person with an attractive photograph who you don't know at all tries to talk to you and talks to you about suggestive topics.  Be cautious of anyone you meet online from overseas.  Learn the signs of a relationship scam. Know what to watch for.  Never send money.  If you've already given them money, don't go overseas to try to get it back  Always confirm their identity and their legitimacy before going overseas to meet them.  **Section 2.1.7. Scam SMS from your bank**  An SMS arrives at your mobile phone from your supposed bank saying that there is an error with your bank account, and you have to fill in a form.  A person pretends to be a moderator of a social network and asks you to give him your password to fix a problem.  On a third-party job offer website, they offer double the amount of money of a normal salary.  When you try to make a purchase from an individual, he asks you to pay him the money before he can ship the product, or he cannot give you any shipping information.  **Section 2.1.8. Lottery scam**  A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery. The recipient of the message—the target of the scam—is usually told to keep the notice secret, "due to a mix-up in some of the names and numbers," and to contact a "claims agent." After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but will never receive any lottery payment.  **Section 2.1.9. Fake charities**  Scammers impersonate genuine charities and ask for donations or contact you pretending to collect money after natural disasters or major events.  Fake charities try to take advantage of your generosity and compassion for others in need. Scammers will steal your money by posing as a genuine charity.Not only dothese scams cost you money, but they also divert much-needed donations away from legitimate charities and causes.  Fake charity approaches occur all year round and often take the form of a response to real disasters or emergencies, such as floods, cyclones, earthquakes, and bushfires.  **Unit 2.2. Online security in the cultural world, how to avoid scams specific to the cultural world (fake tickets, hacking, or phishing)**  **Section 2.2.1 How scammers perform**  Scammers can:   * set up fake websites * use genuine websites to post fake ads for a concert ticket and museum pass * offer fake V.I.P. entrance and ticket packages   To avoid a ticket scam:   * make a considered choice when you look at the ticket reseller website * use a reputable website   There are legal ticket resellers, but if a deal looks too good to be true, it probably is.  **Section 2.2.2. Steps to protect yourselfyouself**   * Employ common sense before handing over sensitive information. * Never trust alarming messages. * Do not open attachments in these suspicious or strange emails — especially Word, Excel, PowerPoint, or PDF attachments. * Use a reputable website   **Unit 2.3. Online Security Tips**   * Once you have a social networking account, you can use it just to talk to people you know in real life and post opinions or pictures (better without sensible data).   **Section 2.3.1. How to set up a secure password**  Always be mindful to abide by the site's terms of use and do no wrongdoing.   1. Stop believing unknown images. You should stop believing images like chats and screenshots. 2. Don't click on unknown attachments. 3. Check the source of your messages. 4. Never share personal details. 5. Beware of possible scamming. 6. Protect your financial data. 7. Avoid sharing basic details. 8. Use passwords or PINs with characters such as &, \*. \_\_, minuscule and MAJUSCULE. | |
| **Contents in bullet points** | |
| * **Use passwords or PINs with characters such as &, \*. \_\_, minuscule and MAJUSCULE**. * **Once you have a social networking account, you can use it just to talk to people you know in real life and post opinions or pictures (better without sensible data).** * **Fake charity approaches occur all year round and often take the form of a response to real disasters or emergencies, such as floods, cyclones, earthquakes, and bushfires.** * **A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery.** | |
| **5 glossary entries** | |
| **Lottery Scam:**  *A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing (sometimes including a large check) explaining that "You have won!" a large sum of money in a lottery.*  **Fake charity:**  *type of fraud that occurs when charitable organizations solicit funds from the public for philanthropic goals, such as seeking cures for diseases or aiding the families of slain police officers.*  **Third-party products:**  *refers to any product and/or service of a third party which is offered by or through the intermediary of the Bank.*  **Scam:**  *A scam or confidence trick is an attempt to defraud a person or group by gaining their confidence.*  **Phishing:**  *Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.* | |
| **Bibliography and Further References** | |
| [**https://www.careercast.com/career-news/10-ways-build-your-online-identity**](https://www.careercast.com/career-news/10-ways-build-your-online-identity)  [**https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/**](https://www.emtwodigital.com/5-tips-for-building-a-commanding-online-identity/)  [**https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php**](https://www.interviewsuccessformula.com/job-search-advice/easy-tips-on-how-to-build-your-online-identity.php)  [**https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html**](https://www.lifelock.com/learn-identity-theft-resources-whats-your-digital-identity.html)  [**https://whatis.techtarget.com/definition/digital-identity**](https://whatis.techtarget.com/definition/digital-identity)  [**https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html**](https://businesscollective.com/8-ways-to-use-social-media-for-good/index.html)  [**https://www.techopedia.com/definition/23915/digital-identity**](https://www.techopedia.com/definition/23915/digital-identity)  [**https://www.techopedia.com/definition/1327/domain-name**](https://www.techopedia.com/definition/1327/domain-name) | |
| **Five multiple-choice self-assessment questions** | 1) What are the red flags to spot a bank scam?  A. A suspicious link received by email  B. An official email from your bank  C. An email from a charity association  **Correct: A**  2) What should you do if you're a victim of a bank scam?  A) Provide your personal information  B) Click on unknown attachments  C) Call the bank to verify the issue  **Correct: C**  3) How to avoid a ticket scam?  A) Avoid to buy online tickets  B) Buy only on online official reseller  C) Use a suspicious ticket reseller website  **Correct: B**  4) How do Fake charity approaches look like?  A) They often take the form of a response to real request of help of a verified relative of yours.  B) They often take the form of a response to real request of help of a verified family friend  C) They often take the form of a response to disasters or emergencies, such as floods, cyclones, earthquakes, and bushfires.  **Correct: C**  5) How to set up a secure password?  A) Using your address  B) Using your full name  C) Using characters such as &, \*. \_\_, minuscule and MAJUSCULE.  **Correct: C** |
| **Related Material** |  |
| **Related PPT** | [**SOS creativity Module 2 Online security and creativity what’s up**](http://ppts/SOS%20creativity%20Module%202%20Online%20security%20and%20creativity%20what%E2%80%99s%20up.pptx) |
| **Reference Link** |  |
| **Video in YouTube format (if any)** | Online safety for grown ups, Bristol City Council Skills & Learning - Adult & Community Learning Service [**https://www.youtube.com/watch?v=iCs3aJYXLwo**](https://www.youtube.com/watch?v=iCs3aJYXLwo) |