**LESSON 11: Internet Safety**

|  |
| --- |
| **1. Description Content** |
| Welcome to Lesson 11!  This is the final tutorial within the first level of ToolaKit lessons. You’ve learned so much!  We want to introduce to you some tips to protect yourself from some dangers of going online.  Are you ready to finish the course?  **Button:** Let’s go! |

|  |
| --- |
| **2. Description Content** |
| Welcome to the Internet Safety lesson. Going online will surely open doors to many great things. However, just like in real life, the online world also has its own dangers. Therefore, in this lesson, we want to introduce you to how to protect yourself online.  Below are 3 tips to help you to protect yourself online:  1. Protect your account with passwords  2. Secure your bank details  3. Avoid scams  Are you ready to learn?  **Button:** Let’s Go! |

|  |
| --- |
| **3. Description Content** |
| 1. How to Protect Your Passwords  Why do hackers want your accounts and passwords?  Hackers want your passwords to access to your online accounts to look for information that they can exploit or steal such as:   * Access your online banking account to transfer your money to themselves * Assuming your identify to send emails or messages out to ask money from your contacts * Use your online payment platform to buy things for themselves   Therefore, it is extremely important that you know how to protect your accounts and passwords.  **Button:** Let’s learn it. |

|  |
| --- |
| **4. Description Content** |
| Here’s how to protect your online accounts and passwords:   * Create strong password with the combination of letters (lower and upper case), numbers, and symbols. * Create a long password of at least 16 characters. * Do not use the same password for all your online accounts. * Most websites and apps will not ask for your passwords through messages or emails. If you receive a message or emails that asks for your password, do not respond to it. * Do not message or send an email with your password information to someone else. * If websites or apps have 2-step authentication system (usually a password and then some security questions with answers only you would know), be sure to use the feature to help you protect your account with another layer of protection. * Only register your new accounts with websites or apps that you trust.   **Button:** Next: Securing bank details. |

|  |
| --- |
| **5. Description Content** |
| Concept landing page credit card payment Free Vector  2. How to secure your bank details  Why do hackers want your bank details?  Hackers want your bank details to access to your online banking accounts to steal your hard-earned savings. They can do many things with your bank details such as:   * Use your bank detail to transfer your money to themselves * Use your online payment platform to buy things for themselves   Therefore, it is extremely important that you know how to protect your online banking details.  **Button:** Let’s learn now. |

|  |
| --- |
| **6. Description Content** |
| Here’s how to protect your online bank detail:   * Follow the tips you have learned to create a strong password then protect it and… * Create a long password of at least 16 characters. * Ask your banking service for tips and their security features to protect your online banking detail. * Do not use a public wifi connection to do your online banking or business transaction services. * Do not save your password within your banking apps or websites that have your banking details (if someone finds your phone or computer they could access your accounts easily). * Do not take picture of your credit card’s number and its cvv (the 3 digit number at the back of your credit card) and store them in any of your digital devices. * Do not share your credit card’s number and its cvv to others, unless you are using an online shopping or booking app that has a secure system to receive and store your data. * Use the security functions on your phone and computer to password protect (and fingerprint protect) your devices.   **Button:** Next: Avoiding scams. |

|  |
| --- |
| **7. Description Content** |
| Anonymous hacker concept with flat design Free Vector  3. How to avoid scams  Why do scammers want to scam you?  Scammers want to scam you for various reasons, but mainly they want to:   * Lie to you so that you send them money. * Use your online identity to scam someone else. * Trick you with an extremely profitable business opportunity with a plan to steal your money.   Therefore, it is extremely important that you know how to deal with scammers.  **Button:** Let’s learn how to. |

|  |
| --- |
| **8. Description Content** |
| Here’s how to protect yourself from types of scams:  1. Someone you know asks to borrow your money online:   * Do not believe right away that it is true. No matter how urgent it may seem. * Call or video call that person to make sure that it is really that person and not a hacker who has stolen your friend or relative’s online accounts (maybe their Facebook Profile) to lie to you. * Find other ways confirm that it is indeed your friend or relative that needs help.   2. Scammers can use your identity in Facebook to scam others as well. Protect your identity with these steps:   * Change settings in your social media accounts to ‘Friends Only’ to hide your information from the public, where scammers can be found. * Do not accept ‘Friend Requests’ from people you don’t know. * If someone you know sends you a ‘Friend Request’, check their profile to see if it really seems like them. If you have other ways to check, like by phone is even better. * Spot fake accounts by visiting their profiles. If profile pictures, cover photo, and some new posts are just recently created in a role. Be wary. Find a way to check if the profile is real before accepting a ‘Friend Request’. * Block accounts when you suspect a fake.   3. Someone you don’t know offers you an exciting business opportunity:   * Find out as much information about their businesses as you can by asking for their website, Facebook Page, office location, contact details and phone number. * Do your own validation process by calling their number, checking their website and Facebook Page, and searching for their office location with Google Map. If you can contact a local business registration authority for verification, that is even better. * Remember: if something seems too good to be true, it highly likely is.   **Button:** Next |

|  |
| --- |
| **9. Description Content** |
| That’s it! This is the end of this lesson. Thank you for your time doing through the content. There was a lot, but very important for going online safely.  I hope you enjoyed all the lessons in Level 1.  Insider news: Level 2 Lessons will be out soon. Level 2 will introduce you to some tips on how to boost your productivity, making your brand memorable, and techniques to increase sales.  Please help us to complete the survey after this lesson to guide us on the content you want to learn next.  You can also earn points by completing survey and be able to enter a lucky draw to win prizes.  Alright, stay tuned for Level 2 content!  **Button:** Finish this Lesson  **Button:** Repeat the Lesson |