**SAMPLE Lucy Movie Storyboard “Awareness Video”**

**Introduction:** Each LUCY Video is split up in different scenes / animations. This video script covers the awareness video under:

[**https://www.youtube.com/watch?v=2z9mPh5QYWI**](https://www.youtube.com/watch?v=2z9mPh5QYWI)

If you want only a few selected scenes to be altered choose the according scene and provide us with the customized text and a draft of the desired animation. Within the field “animation description” you can specify the details of the animation.

**Price calculation**: A modification costs about around 100 USD per scene (depends on the complexity of the desired animation). So if you only want to change the logo at the beginning and the end with the intro voice change it will cost 200 USD. The creation of a customized new video of about 2 mins length with a voice of your choice starts from USD 2’000 (includes voice & image/animation design).

| **Nr** | **Animation Description / Notes** | **Graphic** | **Voice (Male / British)** |
| --- | --- | --- | --- |
|  |  | Your Logo? | This is LUCY’s Phishing Awareness Video |
|  |  |  | Criminals have learned that the easiest way to hack into an organization, infect a computer or gain access to important information like account numbers, passwords or PIN numbers is simply to ask. |
|  |  |  | A phishing attack usually starts with an email, an instant message or an SMS from someone who claims to be… |
|  |  |  | …a bank, online shop or even your own organization. |
|  |  |  | The message might ask you to click on a link or download and execute a file. |
|  |  |  | You assume it is legitimate, so you subsequently click the link and login to what appears to be the website from the organization you trust.  At this point, the scam is complete and you have handed over the information to the criminal. |
|  |  |  | The main key to avoid this is awareness. |
|  |  |  | At first glances, the message or the website might look real using a known logo, layout etc. |
|  |  |  | However, detecting phishing attacks is not so difficult. |
|  |  |  | Remember to look closely at the website address where you are redirected. |
|  |  |  | To be on the safe side: you should type the address of the organization you want to visit yourself in the browser or use browser favorites. |
|  |  |  | Watch out for links that when hovered over show a domain that is not the same as the company sending the email. |
|  |  |  | Read the content of the message carefully and be skeptical of all messages where you are asked to submit any sensitive data… |
|  |  |  | … verify information |
|  |  |  | … fill out a form or download and execute a file. |
|  |  |  | Also don’t let the content of the message fool you.    Attackers often try to scare you to get you to click on a link …. |
|  |  |  | or reward you to get to your personal data. |
|  |  |  | Additionally, check for incorrect spelling or grammatical errors within the email message … |
|  |  |  | …or website. |
|  |  |  | Companies usually never ask you to transmit sensitive data via web or mail. |
|  |  |  | That’s why never click on suspicious links or provide any sort of sensitive data. |
|  |  |  | If you receive a message that appears like a phishing attack you can either.  - delete it… |
|  |  |  | - …verify the message’s content by contacting the organization through their traditional channel of communication |
|  |  |  | - …or forward the message to your IT security department for further analysis |
|  |  |  | The fact is that your company is already screening and filtering the majority of suspicious emails. However, phishing scams are a growing threat on the internet and the bad guys are always developing new tactics to get through to your inbox. |
|  |  |  | Keep in mind that in the end, you’re the last and most important layer of defense against phishing attempts! |
|  |  | Your Logo? |  |