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

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

<https://youtu.be/Og9lf0StwVA>

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).

| **#** | **Voice-over** | **Animation** | **Storyboard** |
| --- | --- | --- | --- |
| **1** | **This is a LUCY Email security video.** | 1. logo and text animation 2. Icon pops up at the same time | https://lh4.googleusercontent.com/hbCZGxfiIzW8j1-JCAKt3aYVh_IDzpUSmhBKo3e6u8GoapkphNrQxfmX2uFVyOXGWR75Kv7wJ-GSutRwOgOsgjk6sCbjulX2o3P3I7z1RGdOEMUx4r2j78_Fu1LNZ8fbUQ |
| **2** | Cyber criminals are not going after company systems anymore; they are going after a company’s users. It is important to have security best practices in place, especially practices that include email conduct.  When you understand the most common email threats, you’re better able to set up protections and policies to help ensure the security of your business.  Common threats to e-mail systems include the following: | 1. PC screen appears on the left 2. Notes appears on the right 3. Text is animated 4. Email appears on the screen, magnifying glass move on it, bomb appears 5. Screen changes and lock appears | https://lh6.googleusercontent.com/ToH5zxhumas75WdTwf3szetRCZE302rk1D2ALweO4NxB_3IlFHH4ww2HOWtaUUxtroxLoMFNnUPiWAixrFhujrGzoaok15csnjnlvS2h0qEw5jlCxvEQkoeO5aQXXCSIKQ  https://lh6.googleusercontent.com/j4AOKejiZp-OeIVL4ubGDsn4IkW1FmS68j-5T41_OS0PJkhsA01VXGvK9_HZra8uFaUD1VFlo0af0Y_OU_cmgQl5b3UxdGd79P8t9C_jUC2WJssgAQBq9rFlzM3lVIodFw |
| **3** | Increasingly, attackers are taking advantage of e-mail to deliver a variety of attacks to organizations through the use of malware, or “malicious software”, that include viruses, worms, Trojan horses, and spyware. | 1. New text appears on the note 2. Attacker slide in with a fishing rod above the PC 3. He puts the letter into the PC 4. Icons pop up 1 by 1 synchronised with V/O | https://lh3.googleusercontent.com/hx3-QpNXj-_Sr8fCpdQZBLNy5XraQwS3iORWbMMX02A0l7ZgmS7ojXN1jCvklVEwQtCvHhluSFxqzRwKAvkIsHcsLXZGjN77_7lqaMTMJ8F-x_5rH3hLe-896-oYOrkkcw  https://lh4.googleusercontent.com/k8ExD4uk4FQ9v1FRxjFFm194VXzMcWXRNXmAR8hbZjznHDVOO0syIS12gNGhWXR77xEkOJOWC3lE3MrL04weQKcmvH4X4sywHpOyraQ3UJzXi3drSbbHnaCRh2r3ZiEC3w |
| **4** | Unsolicited commercial email, commonly referred to as spam, is the sending of unwanted bulk commercial e-mail messages. | 1. New text appears on the note 2. E-mail appears on the PC screen 3. Block sign appears on it | https://lh5.googleusercontent.com/PkbIEhJKs1OMJ7_qsQTrACkgwEP1YMnN0og0Jn_FEr9LnlD2ml240IUZhQ9XJpKHzc5v_RFzzp72uI6LjZpu2jQt2zAcoaX5Z5b2L9McBh6D-_jKKC9ZryGAWZTbnD2GDA  https://lh4.googleusercontent.com/k7iNTVlx4YCds81ecToCSkDJPNTodgtA0JGANCK_-f_f6fgteNLERtwaTDr1ipc8Q38e_17nmkc3eFRoZQ_d8-Xu-y8wFNDXJ-2wbpxXfWpmmNUlIhHPux9I9S6FMRU1ew |
| **5** | Related to spam is phishing, which refers to the use of deceptive computer-based means to trick individuals into responding to the email, clicking on some file or disclosing sensitive information.  SPEAR\_PHISHING  is a highly specialized phishing attack that targets a specific individual or small group of individuals to collect information in order to gain access to computer systems, networks and data. | 1. Screen changes and text appears on oit | https://lh4.googleusercontent.com/eY52fPdJqcMm-n9uyDibRs-Z09MGjyWB3CRv6QN1f8XfZmn79fiRUdYZ9z6spAjMi2Wy_jYa6Jo2Hf7BBGtbbykxW85iQuH_Jgv9Zzu7ZEc4-LwWVJi5DPo7YcsedcXCeA |
| **6** | Now, let’s talk about Social Engineering. | 1. Text appears 2. Icon is animated as in the reference | https://lh5.googleusercontent.com/oXeU3uUBo6fSuU9NmeDW3bnwVHRfuKun9aGw9GBPPO6hQIN-0ydDYFZ93H9oOWpvT-9Gb_3qhem37HEuPGEsltiBFZH9FJHxBEnACwgvFdY3zxYb_WucBpICUgxKYi0JDw |
| **7** | Rather than hack into a system, an attacker can use e-mail to gather sensitive information from an organization’s users or get users to perform actions that further an attack.  A common social engineering attack is e-mail spoofing, in which one person or program successfully masquerades as another by falsifying the sender information shown in e-mails to hide the true origin. | 1. New text appears on the note 2. PC appears 3. Letter icon pops up 4. Different threats icons appear 1 by 1 around the PC screen | https://lh6.googleusercontent.com/r7nf_gxQ1qYguluw4QxThC8AvJ7FVXK7r8TiOpEE2Spn-4fyRu2md9j0syxOzlocXLmcgdLayPgHdhXP1UzZGMD44klypzFA7r2bzGTgBfyxPpTM8FByoxzrhmbn7lI5oQ |
| **8** | Unintentional acts by authorized users.  Not all security threats are intentional.  Authorized users may inadvertently send proprietary or other sensitive information via e-mail, exposing the organization to embarrassment or legal action. | 1. New text appears on the note 2. We see animation as in the reference | **https://lh6.googleusercontent.com/t9TTV_heQnANsdAWqtua2kiR0GXRURoLPHasC7Dxx5R4A38TvHgCAecZAYU9pCFhu1Y_2etjDRT5yydgy5rqt_F5PqrNCLSs34bQhI71vMddsVGDKAhKt78jLFXb7IR3hA**  **https://lh5.googleusercontent.com/9w4WxWKkMoHgVdXULfD2_oBkxMG-V_uclXb02IhbU8HHo7XhCeKBdrFH7YVB7HuHcpveIcOMWPRe2GKzWpgVyO8zISP2U_brDnUyJIE8XaeRfQUfwAMk6GspA3lzJZDDHw** |
| **9** | So how to protect from the common threats? | 1. Picture appears 2. Text is animated | **https://lh5.googleusercontent.com/OBNdrcSbG4HrOBb9u9KrEq1_cc4U2-TxrXrbYplRFrjFusxi-R-mHJbA57wq4njuroupt7Iqx97rj95tj-9voUb7szNA416ceemRYdYSvYnX0mICibVyCkt_LN1x6KPnQw** |
| **10** | Avoid using a personal account for transmitting company data. Make sure that you don't risk your company's security, and your job, by transmitting sensitive company data via your own personal computer or email address.  This includes using your personal email account on the job as well as sending company documents to your personal account. | 1. New text appears on the note 2. Two PC appear 3. E-mails fly from one to another 4. Hacker appears above and steals letters | **https://lh3.googleusercontent.com/TP7D6XGnGtYk02h7AAO08PAmv9AWiKmkzI5ITMTvL8F0RcJzNcpUyAvv6338fk-pJUTGGl3QeM5IVP8a1_xRWJgwfBaIxczBa8Ovckcao_-vuS0n_q_G-n2uPCPPbukuKA** |
| **11** | Your company has a right to see everything you send and receive on your professional account. Assume that all your emails are monitored,  and refrain from sending anything you wouldn't be comfortable with your boss seeing. | 1. New text appears on the note 2. PC screen appears with an eye on it 3. Emails fly into the screen from the left side and fly out of it from the right side | **https://lh5.googleusercontent.com/_9Pub-6cAkujSt4FsMdSon0Y5xo1RT8D6smBXm8CjFuR2hlr1w3FXOgV1pHcJ1TuEgCswNdLSweVc6iaULTjDhyyhM0saOJWAV0AwfnmL2cvc1qE22D2ph9cCPaCPgVcgw** |
| **12** | Messages that try to persuade you to send your password or credit card number are forged, even if they appear to be from your bank or system administrator | 1. New text appears on the note 2. Login and password are typing on the screen 3. Hook appears and begins to pull up \*confidential information\* | **https://lh5.googleusercontent.com/9olHwTIe1FkEiK0wg5H7hPWHxSzdzOvnNQV0zF1wvpFfxWKMHRwndteJcQVhRybtdHcx4QvLM0RiPDDuvM4orP_9DVdFHhl1SLzanH6Lr4AN4uyH6mB42rDH3rXZkiQ_tg**  **https://lh4.googleusercontent.com/rLuc7AMl3JFZO5quESqd7OC_FMtsFUzxOn0KmroLgKGsaEzWl5UzrLCNLRISL-aSIRwDG0t5GJe1GJNrtuyPpnCJYMW-JB-W5ehtTVUe2XfQsGgnD19kbJYSStXkuSAwhw** |
| **13** | Log off after accessing corporate resources from a public device. Always remember to log off when you finish with secure web sites.  If you do not, the next person to use the computer will have access to your personal information. | 1. New text appears on the note 2. Opened doors appears on the screen, arrows show \*you should log off\* 3. Doors close and lock appears on it | **https://lh4.googleusercontent.com/2XuZftnqxbxa_joEuoTqGi2hKdtBVoXL-dTY5i_W_ib0l6aSKH2NtjaPTuHnPyWWvIsjWTmFz_clnb7wEG13Fg3_4wJ9YUL8hydzsaJE2ULOHZeCW80xf_xQi9Xy6Vbiww**  **https://lh4.googleusercontent.com/qZusPCHD3KvtD14Wq8oYpiwNPwA9ei-wTCHMjYwBKVam35g6HDoQ0xYwQyTTh4XHBaZa0NbI2qhjSVrS2egxHvkiYxG4nxaEIPQbDgxXJ4wHBldjlgJ6tjVQRV4ayjioyg** |
| **14** | When you put a person's email addresses in the BCC: rather than the CC: window, none of the recipients can see the addresses of the other email recipients.  New email users often rely too much on the TO: because it is the default way of sending emails. That is fine as long as you are writing to just one person.  But if you are sending mail out to a diverse group of people, confusing BCC: and CC: raises some serious privacy and security concerns. It takes just one spammer to get a hold of the email and immediately everyone on your email list gets spammed. | 1. New text appears on the note 2. \*SEND\* button is clicked and letter moves to different people | **https://lh6.googleusercontent.com/_EJ4RtHtMpZVXGvWtMo-7l-Myo3SZPNVenDNYML0QEmOmRaePLUFfu5E0Os56KUcReSGeQpFw6BCEidK3PiNJzPyUMLhPY8iR_swx2RH-y2kL0FdzLQ7dO885cVNfJ03Yg**  **https://lh3.googleusercontent.com/80d0NndwnTWg50YU2_rWCiK1brVKJjFgqIIhVpIEZtUsIKg7cXPGZvhmsZqzn9Pu4yXoAfACPMo2VTaL5F7xlCiUrr28vMRi7az-evJFp6sUeNvedyhH6GwL4vAGcGb16Q** |
| **15** | Sometimes the mistake isn't in deciding between CC: and BCC: but between hitting Reply All instead of Reply.  When you hit Reply All, your email message is sent to everyone included on the original email, and if you didn't intend to include them, the information might be bad from both a security and personal humiliation perspective. | 1. New text appears on the note 2. Letter icon appears and two buttons appear below 3. \*REPLY ALL\* button is clicked 4. And we repeat animation from previous scene | **https://lh4.googleusercontent.com/i54wHGXXWtsBYQhNkv1vBarKmMu2tnVLsYu4qggLmuBeXt_gFlv96EQYczb5P_3YGA82aFH1kjBHaJcpogFXiJV1LjYdWdAKoUulReBtyyhqwXvBDDvrJSC_XnSg7h_JtQ** |
| **16** | Forwarding emails can be a great way to quickly bring someone up to speed on a subject without having to write up a summary email, but if you aren't careful, forwarding emails can create a significant security threat for yourself and the earlier recipients of the email.  As an email is forwarded, the recipients of the mail (until that point in time) are automatically listed in the body of the email. As the chain keeps moving forward, more and more recipient IDs are placed on the list. | 1. New text appears on the note 2. PC with spam letters appear 1 by 1 | **https://lh6.googleusercontent.com/hs6ez5jauTBh1mrqQCQiVoHOMYV60DtZQbxnVVCuJxVDnpqHPC2jXu5igy4KUdiBFJC8dI7oj9BgThntXtLkpplDBfAf71HpLHmPSC6M9V4Uy7ECjhD_PsrxgFvZ6O62sw** |
| **17** | Just because you delete an email message from your inbox and the sender deletes it from their 'Sent' inbox, does not mean that the email is lost forever. In fact, messages that are deleted often still exist in backup folders on remote servers for years, and can be retrieved by skilled professionals. So, start to think of what you write in an email as a permanent document.  Be careful about what you put into writing, because it can come back to haunt you many years after you assumed it was gone forever. | 1. New text appears on the note 2. Letter icon appears on the screen 3. \*DELETE\* button is clicked and letter flies into the trash 4. Check mark appears instead 5. Box with letters appears behind the PC | **https://lh4.googleusercontent.com/hBFumSDNhcrPdsmtGAwIB0BaB3hrbolL_OUFCIkbw7ave9aJBX4AJnEB951Rf0W4_0Is7s8jN0PsSCHzHXTXMJ7WBJtPKudAdtlbavAN6G_v_2qtzB-0E-WyRkR2q66Btw**  **https://lh6.googleusercontent.com/gH6gSrbfMY7Bwe78BYwtMVDeIDUATdQyS2J5sblfUoA2jJsJyWNghosWsgdYYZIUDSFbO_E8wAAwz5jRLXclYwzj8pjGwvn7nomCh5jdhVXYoNXSUqhhhjgsbsoH7TvTRA**  **https://lh6.googleusercontent.com/d83y4s6uoIyqQh_i7TpzNIxiIp148QA_TQO32L6gGZyFjTeg5HNztLyIuKyeUJ3b3hcUQMsOjb7CpeDlTqTurA1XSYkp6S45U-7hDL0jbXyJV1gdYzQhypP3iXe7L1xJFg** |
| **18** | Don't click on suspect links! If a link looks hidden, or if it comes from an unfamiliar source, don't click it.  It might take you to an unspecified location and possibly inject malware into your machine when you attempt to download the page.  Be aware of any discrepancies in links that look mostly but not entirely familiar, such as "Amaz0n" instead of "Amazon",  and any shortened links. | 1. New text appears on the note 2. Links appear on the screen 3. Check mark and question mark pop up nearby 4. Stamp \*SUSPECT\* fly on the second link | **https://lh6.googleusercontent.com/aV_uSn7O6766EfJMYhMbvQDZEjfazZyAQpNBcZXqBCI4Dy-G35izsWZOv4YQXrd88zlQxzEOeg60Wf-XnMgZV6f2ij8t2tlFHKJTcJGW9PLznKDsfXzgVqvQhGyG1iWCJQ**  **https://lh4.googleusercontent.com/Omwm2XcRvr2tkT-iO-twHRJKDI2cQgoBN_IfNu4CK5UrSjiPDGNgYuCSHj0Yv_KhKZLFo_b8hTuTvqnVC29EtQ-GQ2UC_fneBF5vlpF6i2eZrGBcSAT0oc7acrm4AjHFgA** |
| **19** | It is important to be aware of any emails received that come from unknown senders. Each email should be treated with caution.  It is a best practice to avoid opening any attachments from unknown senders, especially if they seem peculiar or out of context. These types of emails could be malicious. | 1. New text appears on the note 2. Man icon with question mark appears 3. Letter icon appears nearby 4. Envelope is opening and \*viruses\* get out of there | **https://lh4.googleusercontent.com/D0qxAm2TxzQEY4V2EmpAq0XQ16YOyNj_FTU39D2ynOwxfORpIWXJB6movdJmvRJBe9EVXpFLSuV7sjTflC1CcZOAyWOL7shpciL9SFLQlCBB5HlMaGa-76_6w9zTmEPTCg**  **https://lh6.googleusercontent.com/1HlbvO-kxuPc5bFzt6nU2zfZjgDphnrCGCoHtZEJJY_SMHu0gk71sDe91RwnUGYvVSlBGN1Enpz5pJBewjimYdrVbGhtENAFDErjTA7vtlEdD3VCw0KJWe0ZwD3WuMjxNQ** |
| **20** | Spammers use a wide variety of clever titles to get you to open emails which they fill with all sorts of bad things. New email users often make the mistake of opening these emails. | 1. New text appears on the note 2. \*JACKPOT\* icon appears on the screen 3. Button \*CLICK HERE\*  is clicked 4. picture on the screen changes | **https://lh4.googleusercontent.com/IfBPfmf10D2vICcsdSidtQhiiZE5xOpjj58Bv2Vz-z3V-L89X4sDtBVyXTI-Pbyk9DSkotVrwZH2gHE5lGfB7meSKLi-LIjaG-E4vrI5XwSwGClYIvBNfWAobhntUopajA**  **https://lh4.googleusercontent.com/WK2VPo3BvcXbisPGJihoBWqnoM4ym959xLmWLM0l2vsdrjN4ctMCoaAJWR9ofCK61tgdTiHhQZsejL6tcT12K8cc6F6DafAnbiAJLJgSLLUcAbrkBawisZATmgNI8xPYJg** |
| **21** | While never opening a phishing email is the best way to secure your computer, even the most experienced email user will occasionally accidentally open up a phishing email. At this point, the key to limiting your damage is recognizing the phishing email for what it is.  Whatever form the phishing attempt takes, the goal is to fool you into entering your information into something which appears to be safe and secure, but in fact is just a dummy site set up by the scammer.  Assuming you have already opened a phishing mail, do not reply or click on the link in the email. If you want to verify the message, manually type in the URL of the company into your browser instead of clicking on the embedded link. | 1. New text appears on the note 2. Envelope slide in from the left 3. Text is animated above 4. Block sign appears 5. Envelope appears again 6. It opens and attached file flies out of it 7. Block sign appears on the attached file 8. We show opened envelope 9. \*REPLY\* button appears below 10. Cross appears near the button | **https://lh5.googleusercontent.com/7t6obWFtnQbp5HWu0jEMD__TdcwK0lidahr78_GlBmi8XvWcgQ2Xmzhn3X1QGJSvs9H7rWi8NWw_lfWIdVqGUgPS6sZRwvqZaLP4zSPJAehnH3lW2MrDedtQpPc1oF7D9Q**  **https://lh3.googleusercontent.com/5lGRtSIBugFkmDJva5mSHSXbtpOTddSpmtDylnDlgyl8dsrmLDeEoatxkdY-3zNZaXosbgqdc4ws1rE2r06NEYWq49oyQLvQagJTVEgZitx5qN5OG2dUcCcC96ocSX8lgg**  **https://lh6.googleusercontent.com/hROOnnPSVCAFQC51uKkxDyIS0aFS-JLZqbtLUhvHpZHV74z3uUBFrW4KH_IWJvR377CMKT2BDx-GBzWXsG649mRaKo1J5WnuAllHmiwJZimhDqGZA1dP9RCxok8JOGxzMg**  **https://lh4.googleusercontent.com/bs0FleDjDhMCCeVLc4B0hrZwzqF9wVsDahpsqCIAP5i9NR3fDavFCZOetA4G6Qg1BUxmRlH9I267VPRZwPDhjlofilmY2dQbzCtH0FOWMsRaIrY0seREHWYe-Ovmg9e2EA** |
| **22** | A common technique used by spammers is to send out thousands of fake newsletters from organizations with an "unsubscribe" link on the bottom of the newsletter. Email users who then enter their email into the supposed "unsubscribe" list are then sent loads of spam.So if you don't specifically remember subscribing to the newsletter, you are better off just blacklisting the email address. | 1. New text appears on the note 2. Letter icons with buttons appear 3. \*UNSUBSCRIBE\* button is clicked and \*SPAM\* icons appear 4. Screen changes and cross appears near the letter ( showing it’s better to blacklisting the email) | **https://lh6.googleusercontent.com/ZMNiQI7l0WEfUVddbXZVLV02ZYKWKX4eC6jWsojyrZsNR_QUNrUG6r_7npXUVPZ0NqI0orzquu3xDpFQxf98rSit5hXWcQ_a82gqTlPwYM2CHrLAiTLFHfXrKJ-UQNyckw**  **https://lh3.googleusercontent.com/wqjhjxKiFwHAeLiCRSrqlrEfXDBiMrCGSeYh6VS91ze7pdb6LeykVpyAMMXZxzmWXh9UDoleusQfLRJHMOlZVug7RNKQDspkJAKkSIs6vP6rd0iJ_R1UOZlzTy7JNKv4Kw**  **https://lh3.googleusercontent.com/OF8PdPkrWXt9xWpwjZWK1TgchZFn5KvwUrZUdsxOEcrEQefM1eIwpv13RheKZhLD3kzTHU6ENcSpitw-2H4J99fh9A-YKaJLSFVHVBkfTRQmZXIJ0PZa8oOdJ5aZZLfuUA** |
| **23** | Most new internet users are very careful when it comes to emails from senders they don't recognize. But when a friend sends an email, all caution goes out the window as they just assume it is safe because they know that the sender wouldn't intend to hurt them. The truth is, an email from a friend's ID is just as likely to contain a virus or malware as a stranger's. The reason is that most malware is circulated by people who have no idea they are sending it, because hackers are using their computer. | 1. New text appears on the note 2. Letter icons and friend icons appear 3. We click on one of the letter and friend icon is replaced with hacker icon | **https://lh4.googleusercontent.com/CY4CK8g1XE-SdjIrDJ7Mm6miC5RbJOjzZATuheUMymgbA7R5-wY9RNFEACmjceng4CK3RL-74O_o7OVExiX9SW3oVl2ljdGAdU2mq_Vs1LpU630rUsCv1xNQbuRifdPrkQ**  **https://lh3.googleusercontent.com/Wp_Q4VT-RT4FV0GcdF1eywBPlvVqzogW4aHLP4wirbpaKzZovP_iZzxv6DRaJ2kYRLrH-wvaMZ1rIKusAhZmJWrzZVeJwjsnoxZgxrDUapAp4YQ_OsvKMX7GCBXrWQ_P4g** |
| **24** | Malicious spam could even come from an email address spoofed (manipulated) to appear as if it is from someone within your organization. But one click of the mouse to open an infected Word document or PDF, and your PC may be infected. Often these emails are disguised as shipping confirmation notices, alarming notices from banks, tantalizing photos, mortgage scams, fake news alerts and more – anything to raise our curiosity and get us to open an email and click an attachment or link that only leads to trouble. | 1. New text appears on the note 2. Monkey with binoculars appears 3. Speech bubble appears above 4. Text is animated | **https://lh3.googleusercontent.com/o-oO33Bg-rB35XytzSmd1y1gHBW_6ads_DlO9BcezmwwbAgUTcRBPd7KsGKCIjdlovlSmCMzFAEITJqJopuaXifhqJ0zBqfPKL6lLff39AnrK5qdsKsooZC5zMJKRILvkg**  **https://lh6.googleusercontent.com/d4DkjTJDwNekZDugqDNv11YM9npagiGHYPPU95INhONdSX7HShMY35LZYq0Ic0A7vlq_hOeNPHYSKqtopk7eJpj_QpbptvS1OmI3FohwdxbOltBet1iKZQgrbiaRVBC70A** |
| **25** | **Keep your data safe and be cautious!** | 1. Image appears 2. Text is animated 3. Logo animation at the end | **https://lh4.googleusercontent.com/GMDcT1bb3fBF47OAe6odoTbDGIsbdIMvu8vO4u3TFb1AK6OlpZBJBvD2670QDUmjlnwejuxBn-fmUy7AlU9sTEFGLljsd2hHsIDjnUrNMzF4-WexVaQqO0WQzoPloK07mg** |