**LUCY Internet Usage**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Animation** | **Storyboard** |
| **1** | This is a LUCY security awareness video about secure internet usage | Symbols with text for secure internet usage and secure social networking appear one after the other | https://lh3.googleusercontent.com/gVDi3vTaIjb-iLPfP1_wrMhrZ3kP75cq_6VqijOrzH4dV7isCxnVu70XDHlO10pYwzJGnfZnn-0Cx6VcNJ4icaLxpdamUQcmWvIi-m69Zvxc9iSaeiopCPrm9RZn0mpoxNge9XtC |
| **2** | Constant internet use increases the risk of infection by viruses and malware, leading to potential data loss and identity theft.  Here are few tips on how to stay secure. | 1. Malware attacks pc, data is stolen… | https://lh4.googleusercontent.com/8l9SXehdJSQuF_ia9H6wtaHas1x4I-euKzt1EP2fvaA-Vk0YrXWNV55I0pRuFex4-DhTWFCDvfisD8U9a-SH8844DWvlkai8EFhC4zGxNreSyWJ0ASSZlluYlD2jpAdK3amHA6wShttps://lh6.googleusercontent.com/4WVAe6H6LWVL6SJMlcKmb90YGVqlYnSVb4VBMxKGefnQK7bx6OrQKB5u0Z5JEcAz2DKDN1aMn7cA0PCZAYdmWgzk7KDNNG7gOUzQGohVwADSSGOEJVjpAx0b07Y8gdg07_hmuIU6 |
| **3** | **Tip 1 - Avoid clicking on everything.**  There are very few ways for you to get infected with something online UNLESS you click on it yourself. This means you should avoid clicking on banners for offers that are too good to be true. Beware also of misleading popups. . | 1. A lot of banners appear on the webpage 2. We click on one of them and malware icons pop up | https://lh5.googleusercontent.com/NA9jQ4yczsFsriE5WEu8rE-tLKADYrQxl60r0KQ1HN9ofhSDDA7hEiP45N-MlWkvSdbBG5TaKhhSjvSfojcXtg3kPfQ7llySRD3IUk2C-xhYUDuR4ayDa3ur3eQeHz_d7SzQ0Tvwhttps://lh4.googleusercontent.com/_Fx-XXBFSbZCpgprobm_lxo5M9ZPHo61MfhbNt2g-sbVMjiMjPiC221v50-G7djTEJlV0YjbeYowAoUjpMpiVTh4Ni7bNBRnlAdGGlOrapCDOUNpazFgtIuSwCC407ypIzpJW0gE |
| **4** | **Tip nr 2 - Don't go where you're not supposed to.**  Viruses thrive on illegal sites, to safeguard yourself avoid sites that let you download copyrighted content for free. | 1. Show sites where the user downloads iligal movies, music etc | https://lh6.googleusercontent.com/03SbF0YeHFFE9Cf6XJg7wJ58q4g1QNudmla8iyncOlcZuBRXhFIDRPjdKxzyYjo-7WIMIERwNwmDdiH29O-vQzpHSgHaOWpI5l09pBkxuNvwXG55yNX6Adoz05wgUY5MgjZGyC01https://lh3.googleusercontent.com/9FGlkCmGdvpNiMpYxvkgtLz7-JiSBzLJKeXBa3NhPTKWttgXJLXYAUIchMvdVV_Ypl2EKT9Gfy38qzvw4rSDHipGZQeyq2jN2tLlQ2LiFYjIgLjl3l9ROdgllLVRKvMnzgVa6MUo |
| **5** | **Tip nr 3 - Be selective with your downloads.**  Downloading extra programs for every task you want to complete increases the likelihood that you will download something malicious. Be careful what you download. | 1. Virus crawling from behind download link symbol | https://lh3.googleusercontent.com/OBw11IlTyIvdLIDCVEzIUvnrQKDHeAB53IPHuDEzdFuH2_rcP4bJyC-Ii_NEitozHcMm8vW8jD75ClsOHWXy58a2pUoyn0hM_9f7e-_Yub6z80PF6_SGXi9JkTTJcLMVDJ7h2d51https://lh3.googleusercontent.com/hn2vuvVfp3YwrE13Rj1cFS_e0tdtHEyTPzsNSmXeNsTgvrMM6Tbh3QrZt5W9qs1w18EhJXkLyLRfwkuFpCllvMKvFKerlV7Y4l-6b8uPEVZfq3WmEuEONn_midYdLlZPPa5rgfyt |
| **6** | **Tip nr 4 - Download from trusted locations only.**  When downloading it is always advisable to try to download it from the developer's site as opposed to a download service as this is safer. | 1. Original Adobe Website appears and mouse highlights the original address | https://lh4.googleusercontent.com/1UFwj_drGISxCe78gx4WK9KPjpxE0mrdrWVBkj5LEfC3YclPVKWWtcnJeYGtQgIQon4f7aW6VfVdd4d_RNwW4KTK9LkvnFcxHEPqH_eNRZYo72UJKlwA9Z9Sr-xod0kI3sFRBRwe |
| **7** | **Tip nr 5 - Always check the site's name.**  In other words, a site might ask you to pay to paypol.com and includes a link on the site. This is NOT a PayPal site. The misspelling is on purpose, and used to lure people in. | 1. We show \*Paypal\* webpage 2. We zoom to the misspelling, it’s highlighted 3. Block sing appears on this misspelling | https://lh5.googleusercontent.com/pGr0WmY-dtxN_0KRxk9nVfFdohyZm0VERMgmS2WdoBliEvcC9WLY0pfTUAAlEVvCZrD9fMDNkWNhdHhT1Ir49669OZT9fwQMvd_Mw-a3qKcENptXJHZP6C9LQDFAAdtFhqa4Uj4Rhttps://lh3.googleusercontent.com/wvcMPH9ROSWOt0g4D3s2GyekANYdfpmEDYlUpJOdj8RNOOH1RsdtHa4trGev9xguRU7yNVuiZY_8eA_TnksDjvQdwqu-i7vxufOCiLozl3ybvDgn0ELAnZqIwYDPX1OfzOO8tiDP |
| **8** | **Tip nr 6 - Don't open anything you don't trust completely.**  A virus or worm can do nothing unless you actually run the program that it is attached to. That means that simply downloading a file does not put you in any real danger. If you decide after downloading that you don't exactly trust the file, avoid opening it or delete it until you can confirm its integrity. | 1. File gets opened and asks you to run. 2. Virus Symbol appears 3. Block sign appears | **https://lh6.googleusercontent.com/3mMEIviWDvFZMzaiVsEoc13DDwChp7msAQ1pcP_UtdgAqAC9aCzvfjwBN0y6ka_JjomNnLIGBFMCspRT10FE0d1bpfrtdGkoxYcms0zJ04zYYXNFRydyjUZFkAlOCqRI1X9JJIHehttps://lh4.googleusercontent.com/aBqPLC4TL39a1hId1cMgTWPtyXPS9GRvMYr8RwFIFdQVAO8Rs6OxyjqrxUlp85EEcddprjaxUDRTswWpS3eiJPbvySfGCRcnsiEwhjbVstRlv5oK2H_wfL3R9pc27XjmCfMVg7eu** |
| **9** | **Tip nr 7 - Look at the file extension.**  Be very cautious with executables. Mischievous files often have fake extensions designed to trick you, such as ".txt.vb" or ".jpg.exe". | 1. Different type of executables appear 2. then the Setup.msi gets extended with Setup.msi.**txt** | **https://lh4.googleusercontent.com/wDWtIJhT51E-_IN-2auLIroMPfL2hvCXGQh_wSHEOVw1yztuRMqYYP9i3deAklPpl3gTFO-F5yVur116dKNUVI8Y2qwgE3tU97WRSMbQHJE7MXrF1X5_G4b8LMaq6LeLQkvgToN0** |
| **10** | **Tip nr 8 - Don’t expose your e-mail address.**  90% of the time when sites ask for your email address, this is a scam. You might end up receiving plenty of spam. Don't give it to any site, if it is optional. | 1. Download button (below some file) is clicked 2. Pop-up window appears with form where the user is asked to provide his email when downloading a file 3. Block sign appears | **https://lh4.googleusercontent.com/BpZbK25E_Q9Io0dIo6ayXCNicdQZNoY2TiBMuiTDg1XqkJ0zY1cO9giaWI3bkHXM7Fejz_pOot2MHIcDGLOmH-LH7lKewe-YscCtZ45skOXzjwBG52aNZsAHVUzV4hrf6PQSLDJehttps://lh6.googleusercontent.com/sT0I0ZVAPvtvdmP2WN_iO4R7tdyXyX9xilfjVkbBkxs-sVRskJam9AQk3XEEQ-TsXEQtAbyqvwazym66xG0DFpwnhI8CCP1qNYxrREFg7UvChxurl6V-tGrX1nZwKI3Mej91d3nB** |
| **11** | **Tip nr 9 - Check your statements regularly**  When shopping online, watch out for suspicious charges and check charges against your records. Call your bank or credit card company immediately if you see anything suspicious | Show a suspicious transaction within the online statement of the credit card | **https://lh5.googleusercontent.com/ukXpf5EoN1tWjShJdyl9pGfaVwg45Pc6v0JHMSVeYoCjeX6-ooim1kF8Mst7IrCEuu_mkR3ibxOusLm_Sq4bSOTsrdJXY0XOXbZ6FFtf0_mITbrubVNBhMywN_gljUF4Ur83e_d7** |
| **12** | **Tip nr 10 - Be cautious when using public computers**  Many websites leave you automatically logged in after you close the browser, leaving you at risk for others to access and use your information. Always be sure to log out of accounts before leaving a public computer. | Show user surfing at a public place (coffee, library etc.) | **https://lh6.googleusercontent.com/lp00nzqgWowG907_XxbYj_5fVS7NFFMlvJlp9cqc_FJPmnO3TOoWPPBA4fr4P1I9SD2bLZtMFolvUf66FyGJmfE36nxrFuUwH5q4HQhxD-6qawGVcRnskwG7DsVcBQ_AIrtKz_kS** |
| **13** | **Tip nr 11 - Research the company's reputation**  Research the company's ranking you visit online by looking for reviews of the website, but be suspicious if the reviews are too glowing. | Show a rating that is 100 % positive among many thousand users (which is very unlikely) | **https://lh5.googleusercontent.com/iqbIwKt7bxFTMaFEsvGLdDGiFzCPCyPOjV438VY-jx6DG_ko-14HyY_u-3SO_nog8PUyv69o97hED-mYXWpIa2q1O9bt0vxgAoergL0CB_JmiYe5X-txSsKZjbIqQEaxjZdyWhee** |
| **14** | **Tip nr 12 - Use encrypted websites when possible**  It is best to use https:// whenever possible as they are secured. Most important, never send bank info, credit card numbers, confidential e-mails, or other sensitive data unless you’re sure you’re on a secure site. | 1. We show similar image (general website) 2. And appropriate part is highlighted | **https://lh4.googleusercontent.com/1kmxI24yBbRAPGB7j8OVJiliJMsvBIrg3qu_p-B11dfVE45vDl69Ddibd43_JrUbBTrueUH3xY27ZRP5Tbd54nVpxSZoUP17iFaA__18C33rLAQ1vmvLoMUgczLcjCkzQQSiEYnK** |
| **15** | **Tip nr 13 - Ask yourself: Is your Internet connection secure?**    People don’t realize that public Wi-Fi – such as connections offered in coffee shops, airports and hotels – are often very risky places to do important things like e-mail, banking, and social networking. Whether you’re using a smartphone, laptop, tablet, or a public computer, it is important to connect only to a network you trust. | Show a user that connects to a wifi hotspot called “free internet”. Once connected, some malware appears from that hotspot | **https://lh5.googleusercontent.com/nJTcGYdbsvZninyhALDdsgGu1Fbw1Bq4PYwVlm53PHhOj7CiM4ebIvtKR3DhZ_vI95Ltb1YwBGnsmg6UmZKRejS-6TxBib1ubBehPguP42ptDfNtel061vVgjQxLOahpdrwU4Os-https://lh3.googleusercontent.com/pFti0XRAech5rETRxFTdp49BUZ3Eo6_zyBrav_pgdwAstmP2oVXQJR_KdDGK7BNGBt_SMpS2nIaCVUWCcHGw-Q_0f5bznCDdqdhE-RRuRb27YkzvByBIOaLoP7wb_LA2ENhlpwuM** |
| **16** | **Tip nr 14 - Do not give out personal details to strangers**    Don't give your full name, address, or phone number to anyone online that you don't trust or know. | 1. We show similar image 2. Block sign appears | **https://lh4.googleusercontent.com/3RTLHMw5ig5zHKw7SyBASsd4eXnarUskKUuIVjPYWwQ5LUZPotVI4HOtKGUXm0jOV9tgaSVyIyvcDZaeKC-ZJO2KGhhIBGONb8JoSAOeWIPnEdxIGd4twouClJAw04VI1h-QbrBLhttps://lh5.googleusercontent.com/Z3k-_4MFe7Ja5m1AAmTm0ljnd_C2IzOOtj-oi3uVfvIuuQQNZ6Ed7V9UK5FJcUkFYkiu5xCk3P6I0wkZn_SckcreZpCYV8u0zH5jIiLVBCPwf-x1-_ppHBG8Kh2KdFIZRfgduXlT** |
| **17** | **Tip nr 15 - Hover over links on a website**  Roll your mouse pointer over a link to reveal its true destination. Beware if this is different from what is displayed in the text of the link from either another website or an email. | Show a mouse hovering over a link called [https://login.secure-banking.com](https://login.secure-banking.com/)    The text tat appears when hovering over the link is completeley different (like<http://private.webhosting-darkuser71.com/passwordcollector.php>) | **https://lh5.googleusercontent.com/OC2pTD4sf0YZKoSnCk09TdamZVF934_uhdaL0PVC6KNQ_mzB3Wf7PFdyPqrM4wzbL2jolRKoFqJjpEVpdxw96neeHbx3Q5NJB1jWfPJquasjjegyQOxyT6p_McIO-jk51PXzcCFJ** |
| **18** | **Tip nr 16 - Choose strong passwords**  Passwords are like the key to your accounts - only the person with the key can access them. When choosing a password, you want to make sure you choose one that is unique, strong, and not easily guessed by strangers or those close to you. | 1. We show general website 2. And then zoom to the password field 3. Strong password is typed in it | **https://lh3.googleusercontent.com/d5wplIKV_CfYAQ1_Zsu2ZgghvmPAhfL96v-tzH72iDJz7IKrS3XVj4mivifR1sB3tXjp_XuMkJa81TQdueMRe75THsb0jq_kEXokSkDHv-yhH9EEJSbt1uIPuzZET3vmu6CY4HzV** |
| **19** | **Tip nr 17 - Use an anti-virus program, an anti-spyware program, and a firewall.**  Surfing the internet without a proper protection and updated applications is unsafe and invites spam, hackers, and viruses onto your computer | 1. A pop-up window (Anti-virus) on the screen | **https://lh6.googleusercontent.com/oUtbc1qjiKAWPFwlYj85jb4oAOiUj28rjwaoCuHZjsoSSh9C0sbKNTSdX31-yqvDgQHf3JNjyGGWTyXLxCntL3hBRR_h9nlqUAmcEgSEqkQPvVH23Lh4IQDtrjcPV09greXi62Ei** |
| **20** | Thank you and stay safe! | 1. Text animation | https://lh6.googleusercontent.com/Ghau4m_baZroUCuXWgBe-JHZ1dE7UPaT2eyCec5bPydnNREtiSsAbqaHSjArftaPrhS8FOq0E95poRjJC2t5ABPnjfvDhoXowThrIlfB6XtqKPJfp6NjQwyhN4i-pyocGrzMp4kG |