**LUCY Social Networking Storyboard**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Animation** | **Storyboard** |
| **1** | This is a LUCY security awareness video about secure social networking. | 1. We show the same picture but now there are social media icons behind the monitor | https://lh4.googleusercontent.com/3Onhd11-dly0cDGU3GsI1mi7V1UiVS085KMhTtCuKn4lXflxAyiwVBl6YXuuL4BCU3Xk2ZRFqEeu7gL-p-FqK2_mjM3yrrrvyEvvnIEI1gC3iCyTnekd9HcW96PE3DhgrY0V1KX4 |
| **2** | There is no arguing the usefulness of social networking sites. However, as with any new tool or application, it is important to keep a close watch on its security implications and risk. | 1. Social Media Symbols POP UP | https://lh5.googleusercontent.com/HwSE6nytvvNhd0HGUc1ZPsT0ThrAawQMpuaI65r2xxJQEsmHdsSJJQX3Ky03xMb-CrHuHDXc7DTfPUsAasrq1-fKW7KBluGmHdHjUIip5WIOdNHspyOles37ZtPdX3yLXvXuFSXt |
| **3** | **Spam**    Crafty spammers take advantage of the popularity of social networks to design new spamming techniques week after week. | 1st Risk appears      2nd Graphics: Mail Arrives with some Spam Info initiated by Facebook | https://lh4.googleusercontent.com/kYJJdimawsXnPFYNLdjnMDG5E274AUnMmUmArnHJRXIVUArVK5kc7e8mIcjuaZiXGb-Npg6BkDrAkX9aKSo29_eAa8cUWd6kQCmpyGozIe-8r16aTsbb8iD-4HVt31dyM_ccecAP  https://lh5.googleusercontent.com/FMKbDoT90dxvQtrcnsV6-TAvlMBJvU-ISEJBfla2DCLMdpBdnWhmGvVPadQCusOva438CPmkCI79g6UyevxjfHAcnEgqbBPFKL8CYWJwZF6LvRFDxrXkauUNv3IMS72QhQd6ik_N |
| **4** | **SEO attacks**    The SEO idea is simple: utilize keywords and links in such a way that the sites are ranked very high and appear in the first search results. Similar attacks can also happen on social networks. This makes it easy for attackers, who can automatically grab hot keywords and include them in their spam messages to get a better listing. | 1. Twitter Messages with shady links appear | https://lh4.googleusercontent.com/ubmAk1xsbGXuL54RGozbOup-99mnZj9kHhpnuktqLMslYXIxb2gZDZPXL_hhjFuibHPp5E0byDKCGirNzxPsxNpwmccghcUhNHfpDGeyH43u3Tcxbi_80Vez4rm0q0SpgSsi8hip |
| **5** | The pressure on people to get as many friends or followers as possible on social media has not gone unnoticed by scammers who leverage on this to get people's account name and passwords promising them new followers daily. I do not need to stress that it is obviously a bad idea to share your password with strangers. | 1. Next a webpage with offers appear 2. Next an attacker using your login to Facebook appears | https://lh4.googleusercontent.com/1xDTYK392JnYYizUesxM-ExyJoBWrqRXG95DF2kgf0CV0-NJ2B_C6kfEqHlqnE5zliKpgHC3xHkyhD_Zt7v8TIL96bswB6vSYpV08UB2zWEF8iNBGr5kwY6pvO9aHEW7JVgUKTWo  https://lh6.googleusercontent.com/j6TLTQDXrtJE9UuSGyUdKf1d23TW25adDm3pC0iNH9VZFJUwUXm8UfWfjSuqQmjo1J0vihh6HFmEOnsr2GKubGyae8BzSz88W1OCffeg991Kx2c47OeN5sFVAG3rbPLBB-q3sfq5 |
| **6** | **Impersonation of celebrities and friends**    Scammers find it quite easy to register new account under the name of celebrities using publicly available pictures as profile pictures. This accounts majorly contains advertisement and SPAM links. | 1. Some Fake Celebrity Profile with SPAM messages appears | https://lh4.googleusercontent.com/ZIn7cFisOapHVT4NKtR0q0jjRlw2oSHINU5ARMqFlBjjxtIR1ZeBgRqMjzdUL6HG7PTgoicamHt0n7bgm0edcFB7oYnt5Y1hcGAPb326CHYOWtcc1Z5LOm3Y4raPps74HZvflOPs |
| **7** | **Phishing**    Phishing comes in many different flavors. A typical trick is where the user is presented with a link to an interesting picture and the question “Is this you on this photo?” The landing page then is a phishing page that intends to steal the passwords. | 1. Profile Picture appears that links to a login which is controlled by a phisher | https://lh3.googleusercontent.com/CdtgFsKXprKVyWyt71OleztG5h4y0hhkFA95CYtCofEmqhFJHYXAxLQIkXWLf78LYs-6PPrzbTqfuY_lQFHvwdEucWuj66Jltr1P-RyoEtbft-TSEIJ6ubUywQyoXBQZBfRvuRdH  https://lh6.googleusercontent.com/ssPhKdjDVaSA_u1R60UmcWpeZrLJJRoGcs9AhVA3QwIJTY5bn2wca_6HLtfTm8DULgFRD0bQPSP9PVGkUX3zqtpe5Ib6RC61ofCTqWlDN1el5-IB1_OOC-vooGNSlICWMfu-V9ks |
| **8** | **Apps and widgets**      Some social networks allow active content to be embedded in the form of applications or widgets. These applications can then interact with the user and his group of friends. A simple example would be a daily joke application, which posts a new humorous joke to the user’s profile site. Some social networks allow remote code to be included, which poses a great risk as it is harder to control what will be loaded. | 1. Video Widget appears on profile page. Once clicked, the user is spammed with advertisements popping up one after the other. | **https://lh5.googleusercontent.com/WlOLpNzmPfBIi546NtTZVezPpwjpyoqIrVFkm5BQuwF_jBlBIwrrkKUGOLcLm343XLtSI0mC9nckawihp0gMp_vU5Rv3Gah1EQY3keZuxz0OS7bdFqphX17iG2O-QL7KLnxn96Dm**  **https://lh6.googleusercontent.com/oZJbkGBeUCHZiISgVjRhQyvdHgISwIuyUyF5BKwGT_Wjfd_GX6wqRCysD9fvp9qxIbMm4ALobdgytSqNwIHjtNvsjnNX53Z7Ulh2qc8ACxxrfvQHx77ryQjBR_lvbZNUpmO-WTl4** |
| **9** | **Malicious links**    One of the most obvious attacks is to redirect the user to an external malicious site which may contain anything from advertisements for fake products, to misleading applications, phishing sites, or even drive-by download attacks  where he has no control. | 1. User clicks some links in another profile page and ends up with malware | **https://lh4.googleusercontent.com/BI1ie-tj9pyR5zOF--mJfNmE-ZDv5HN5HlgTNkbR41lYyCR8tkKF9r1bHtXBn--YpOBj02kTU9uf-KdeVZsI8ctmlf0ZNhGpmB2pICQnuBnRcILv7ZpxvUGJrlh6V67IcZZ7PyYK** |
| **10** | We learnt about risks.  How can you protect yourself? Here's a few tips. | 1. Text animation | https://lh6.googleusercontent.com/7lhaBkJBJ2z_EybgBGyh82UDK9wWJZTXf-t3SmIN2VQFxM7hcMKI-ExgZETcewk79VRwyRD_CivJ2n5yoHGX-0D909xCbaTBN_SeyFly3ahqVIiqtlR4R-TXA9Q4QLRCHqagGdc7 |
| **11** | **Tip Nr 1: Run only approved apps**    Most applications on social networking sites look harmless but there are some that may deliver malicious content to your computer. Therefore, make certain that you only install or run only applications, that are from trusted source or approved by your corporate IT department. | 1. Tip 1 appears 2. Few general apps appear on the tablet 3. They flip over and green check marks or red crosses appear instead 4. Cloud with text \*Approved by corporate IT department\* appears Above one of the apps | **https://lh5.googleusercontent.com/r8NgdhgD4kVYTuSz26C-jrCHwuPy5j8Fzmi0dpKWFVD8Denxv3V7YbTafc8yYBSdOta65-0-_ikStqlQpFf2DyDZiqWOoCY0ZOC6hQQZ45eauslXJNT1rVZ91MtKN_eaQOXz5POo**  **https://lh4.googleusercontent.com/K6-Jiom3EXMKXxMkx_H5LYFIHLKfAKNDq0H0mji8u7Gz01HpBpYuYqcIv-TEjlRixSC8VFBiMju3ql-ZrDLYRg3T9WvhLkwDcuVNL7xAFPM6qKcDzWr8a37mOmxKEYesQdrzl7CDhttps://lh3.googleusercontent.com/Yr__jlCqzxGkOuv_77T1fTM-C7tb5V5t0AnZL7toLgbbScYHvPI7DdVh1iFDgFYNoG7ABmS0OnoAoV_bk9Hm4oAMVfP-dAnEv0JNcQvxIrO_Lyi-8cRZeCXRLHIZnVDtIWI66wCJ** |
| **12** | **Tip Nr 2: Think twice before you post**  Once a message is posted it is nearly impossible to remove it completely from a social network. Therefore think twice before posting pictures you wouldn't want your parents or future employers to see. Protect your reputation on social network. | 1. Tip 2 appears 2. Picture is animated | **https://lh4.googleusercontent.com/HUt3KhKRw9aQwDFhFh_tjSl0SnuxFZJdZ-NXaEaLa-eoqv-rvav6SNTHLyGyQv3SKFy7zhrQaHSIWlCo8T-CgJTrBUIYDafWJIQqnE-Wuv_UMHZHkS-2DOj3Y5XAklyL_2YL-2_Thttps://lh6.googleusercontent.com/4hXx5x7TrERXhDQhXGD3qH1flK2mibdtBjWbkcrmxgQZtM7l-oZQeE0fpq0CnsmAGXPOLjVHSZiPIHA2dp43sn7r9fogrOfmTLs8wgpH7LhorZhQ2yt8-Xmx9zkpUJeCs9ZsEC5n** |
| **13** | **Tip Nr 3**: **Don’t share sensitive data!**    A post like “Two days to go, to the one week family vacation, Disney World here we come" might seem relatively harmless, but you have just told all your friends, as well as all their friends, that you will be away from home for a full week. This is comparable to putting a sign on the main road that shouts “Empty House” for all to see. | 1. Tip 3 appears and a funny example of what NOT to share | **https://lh3.googleusercontent.com/ELSGgbdK6SH2EyhxcSzxkeOoq3ViKfXFTtU3_5kBqTiZPUHHQOCfngoruq6AMXDIsVrfKCCmjCVFSyVRES-8HYcURFEEHWeyJUrcMbbsrgaJLhb2dLZB-ZIbsFeow_naVC4SPsUFhttps://lh3.googleusercontent.com/M6FQBJCJdaEyXYDEEY09yUfdARGQgpQ4P3ALkuzWyMtrNNfdLCC4Boz50e6z2FoE2LRtD6nNubOAbGb4ZQyXuIxoSWD4mELvKWusAxTkd3hms3CcgD20G67VAoXy6AMPcNyhwF2o** |
| **14** | **Tip Nr 4: Know what action to take**    If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. | 1. Tip 4 appears 2. Friends icons pop up 3. Spy icon appears among them 4. Unfriend button is clicked and block sign appears | **https://lh6.googleusercontent.com/qqNhHGf2RiVK8_AEh0NQmkdEI1sGdVYaRXoKWtZ3JXGJUWAnqQu1Bh5b5CH0b_39Jxvyakgi4p5NebPr3FswzCzsYoMZSf8B8Rtp4qa_tRddLEDDhJlGUME_N3Wp6nI541MYJ0othttps://lh5.googleusercontent.com/FZvGgUn8PuVwSnHXpzkXxqxiGKK2iO_LNhCZEQpI3lU97cJzHcUML0K0WmX56BikVycH1N6qdeiq0S31yi8Y9hfd0qi4-sTt6kKgAGt7o1Z8p3w_Y_6sv92BDLVdtXD1p5mVF9Mnhttps://lh5.googleusercontent.com/5UxS9hTInJb7aVJdTDvEPSNr4jXSgrsaZINtl18ZZPQsr7CMtkz1lSmNnTjawzTxuogT46_Hx0nrNEOLep-_YgtL1cf6IQUSB-0E7h6GNlLU8fVzqvtDt_5V5PAWBXT3X3vXtQil** |
| **15** | **Tip Nr 5: Be cautious when talking about your job or company**    Be very careful how you share personal information online, especially information about your job for example, the statement “My boss just laid off 30 employees" can have serious public relations and financial consequences for the company. The impact can be even more serious if that company is publicly owned. | 1. Tip 5 appears 2. Twitter post \*My boss just laid off 30 employees\* appears on the screen 3. Stop icon slide in from the right | **https://lh3.googleusercontent.com/jX_eDFm-RDWroLCF2yrHL0DETxPl6zGi6NQxEdw-zkn7_MLDvjuvPjgUffL87uyEOP8JjKHhxoH9iRtf_dLeP9rhUca_u663qp-_oARQPQdg6zTN-SJ0E_qX0hJKbvAakwwlf1XQhttps://lh3.googleusercontent.com/k9GQgUnQoBacpoaN-tUkRF0SHHVYZdQiYJ2t5ezNFyY9CTuX8_9mTJS5w0eJ_Ub-364JxNj6Vs2VpiwjE9xCTzIlRWCzVKVzoScEiUKiEYuvWFpv6wa9AACw2B3Wg8hS42sfdBVbhttps://lh5.googleusercontent.com/32qYD64HzthGyGJUTa2AuyLP_76kP7Cd4yakY_wtthlEVEPfvJ4MoJa8_Jt62H_cE7z8wieTezx_v651gdo3nWlLmmII3Xkn44K_YcIrH-YUFztXEfIseYVjPE1J-d74Ym7AWxIr** |
| **16** | **Tip Nr 6: Avoid password reuse at all cost**  It can be quite difficult to generate and remember unique, strong, robust passwords. Still It is crucial to not re-use your passwords among different platforms.  Also change passwords regularly and use multi-factor authentication when available. | 1. Tip 6 appears 2. Calendar appears 3. Text \*180\* is animated 4. Bell rings 5. Text animated above 6. Icon and text in it appear 7. Red cross flies on it | **https://lh4.googleusercontent.com/6UqPatA1xvQT9ZVq5id0rISXdEYgE-UypZtdm00SQeZOLqTjb1S2HZV4jUZsjMaU1rq8Ad-pTHco8ZOe2hj3Ys1Ks-mwVHs0PJ7n592dwz3WHDHKuAIq-6SE6ibIh8M4OhdnwHYo**  **https://lh3.googleusercontent.com/kqzD-AcOQo5r93QzQQ1nrPUMAt3-AAow-Q39TY0hL57_IqUUvxVRcVhcXLiPJybhprK8Rg-wNSWeSrVEpTVtDW-aL6Yk1KAOk4G9YnIwg-tzzD3ZJJdTR_Z3od1DLHV1kkLmPa1C** |
| **17** | **Tip Nr 7: Stay vigilant!**    Whenever you’re online, remember that bad things can happen. Accounts, links and direct messages should be analyzed with a careful, skeptical eye. When in doubt, don’t click. | 1. Tip 7 appears 2. Text \*Social media\* appears in the middle 3. Icon pop up around 4. Magnifying glass appears and moves | **https://lh3.googleusercontent.com/oD8Qm2TklgkklSG3hqN1Ik-zQgRnoCNH16277pIv39cUDHj_Umvf9YM3aOjT341Dup0PYQkQxJ6-aW3F8HHLDtdb7ex4nd8OgOfQ5ghGgIT8_zRbkSfrm86sPXaaA7UVaL7Ij-u8https://lh5.googleusercontent.com/d7hNn-NDDikguGr46nxiaN0p8fHkntkAAzH9TuaevKPDPrs4Njc9a8djKvfbPQ4xQZ-_RDePY_wC0fvD70GiGwyzGKPgQsBc2z9YISIIva1kLfHeUrMTCxYDAGSN8MBl4Xt4O67B** |
| **18** | **Tip Nr 8: Curate your connections.**    The possibility of a fraudulent or compromised account sending you a malicious link is increased with the more connections you have. Keep just the necessary connection, only a small percentage of your contacts should be considered both professional colleagues and personal friends. | 1. Tip 8 appears 2. \*Connection\* icon appears in the middle 3. Friend icons fly from the main one 4. One of the friends becomes a spy and red cross appears on it 5. A few more crosses appear on other icons and they disappear | **https://lh6.googleusercontent.com/grnXzIfRHeGOmJbTQOjbBmVGfsf8IIj-W2qdgNOSZR1oNNL5Zgb9aWYArJLFVl99ZBWGHQ9LCuoCGVeFaO_4DiWCzf8a94p9oRm4p82Xcxp8N8yD77dX8XTZfd79qD9NVrzG7Nu8https://lh5.googleusercontent.com/yjMQh_0wKKdUkPJy_DLVUcwXRCituNFPrs3sh3fDETRLAw6r8xShHWiLUQeSD2XJYKKJC-wOFEF7W5OEhUjIOnWSGEZIqDlwNtZtrbo-Nxsb208DBfuCFNKBT8TgM1t9hCB0zzHqhttps://lh3.googleusercontent.com/HI7EP05tffYKNX-rKFO1EPucqbr8SYhqXRNRU-ehLaNCiMzl8YSAE3eBd5pB1MtJtfzIPtEeliKXg9zqs3zCeivnNTTwmkuWTo_QsuFBx6mKfEqUzh459jBQ6W4QvMQhxBH7cMg7** |
| **19** | **Tip Nr 9: Use Social Media Privacy Settings**  Spend a few minutes to tighten the privacy settings on your social media profile as it is safer than the default setting on most. | 1. Tip 9 appears 2. Lock icon appears in the middle of some general website 3. A hand slides from above and inserts a key into the lock | **https://lh5.googleusercontent.com/avbRRjYalZfHGMdxnrkvWY5ywIVOjFReiIq_M99xl8MxmfnYnzdp4hJ7IDM5xge7peKaSXsF3in48Te44k018acPtUKTk_q_ZM_U2oSjsXopCaSWQoQIiKrR3ylVGOLZiHdI4elphttps://lh3.googleusercontent.com/EtLYoxqVFlKTYaBDJ-Co9EdKSQsrPWbovZeugFViTdv4KUHHRidoM9D80jbA3N-b4O4KQRSiI5rUTAsAQTnrUSrjPdn3q5McxeePYI0VfX_LlaiVIyK0wEoxhUueXFpMTe3UdoUB** |
| **20** | **Tip Nr 10:** **Use Different Profile Photos Across Social Media Accounts**  Remember that images can easily be found using search engines, utilize unique profile photos to differentiate between your personal and professional accounts and change them on a regular basis. | 1. Tip 10 appears 2. Split screen 3. Two mobile phones with different profiles and profile photos appear | **https://lh6.googleusercontent.com/shBBe0lNZoMFssgsDqk6QScVw-Y9jVJRpH66lO9oqjRyzIsWxQ2owFlfIZYYNoFESrk8gPgPuJmZYkZckX96IYgLqEqxAanexb72mWwDTCMvDUfPFSvM7VhZZL161dkuSj6hXfO2https://lh4.googleusercontent.com/-_DTtVBjHNs2jDtR3IMLysMCs6PTkGHplXkAN5pR96sgVo3IwTTxDvBYWgT7YESBNLVU2WjN1RdZBqPa04Z9cOFvidDUJ3y-IKDlSLGUh7-6xh3V06hLt_k5ETs8-xCZ6z5EM1IA** |
| **21** | **Tip Nr 11:** **Use Different Account Names for Personal and Professional Social Media Accounts**  Be very careful not to use the same social media handles for your personal and professional accounts. Instead, maintain a professional distance between the two. | 1. Tip 11 appears 2. Continuation of previous scene 3. Different Account Names animated below | **https://lh3.googleusercontent.com/5W5WuVIK7-BpqtK9baIvrBaf_kyduTS2DxUv_jZcBnEM-TmOFlQvJyleUB5H_jGRVuVO3Q26bZGh-ZoetDML1ZEGjqpq2J9puIJrgUwpTMwLN3eMJtQfo7wLMrFA9cTgiDIzPFb5https://lh3.googleusercontent.com/3grPDTSkSKnB3bDNKedxSVyc8PPKAfn57xBxANLruz2DplAH0jJLsAwIrb-F9lJT25rT6IAbsYl6EiWR_cmXOMM6DYEzcnsgSMl7H01fy10skSViNlYSDekgznJyWe2VGoSZyxVC** |
| **22** | **Tip Nr 12: Be cautious when allowing apps to track your physical location**  Be certain to disable geotagging features at sensitive locations or you may inadvertently be telling people exactly where you are, where you work, or where you live with GPS accuracy. | 1. Tip 12 appears 2. Map is animated on the tablet screen 3. Pin pops up on the map with text\* I’m here!\* 4. Block sign appears | **https://lh6.googleusercontent.com/TtzFkdLxr8QXDJ0ALr-Nff_mzMUyNzFQth8u6rBMzI2qfzNlbpmdNus6aiTsx99YIRPDkRokLtezNwMeY8RBf30MQqh3XoScYohtYY9NJfXK_Yb436A13yj3f_1b2d-5PvSyqAYhhttps://lh5.googleusercontent.com/3TxOqVKmY7SiBaSo-zxr3rAUxy_IxbPxOL6EjCeIuloO-dnDaf0dnbzaEKddyyn2m7Yk7FbITIxSkYmyrMhsDybIKNAz7uFY8onCO2JHUUCJ9GcoBJRj02ckvTioYyKealDtNH4r** |
| **23** | Thank you and stay safe! | 1. Text animation | https://lh5.googleusercontent.com/WpC6pGJQgfwjd8jQe3aSlwWnNH2S6Cycb-0iYMiOp4S0rmdBXDyOsuFyseuvwBLEHUPoOfFkpY8PDWAt6Rydiq8nuwmmcnQAlCIx3m7eaDtaA4cngn2w5c-CatNgk5-Mkbps0FWA |