**Lucy Malware Storyboard**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | LUCY’s Malware Awareness Video  *Dies ist ein Malware Awareness Video von LUCY.* | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, it is easy to come across malware. But what is malware, exactly? Short for malicious software, hackers invented it …  *In der heutigen digitalen Welt ist es leicht, auf Malware zu stoßen. Aber was genau ist Malware? Es ist die Kurzform für eine bösartige Software, von Hackern entwickelt ...* | 1. A spider goes down from the top of the screen on a cobweb and goes into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device.  *... damit diese Zugriff auf Ihr Netzwerk, Ihr Computersystem oder Mobilgerät erlangen oder sie anderweitig schädigen können.* | 1. A lock pops up on the screen and gets unlocked 2. Then the lock is changed by the malware icon 3. Two other laptops appear to represent a network 4. Phone pops up |  |
| **4** | As a result, you may be blocked out of your own PC, your data may be stolen for ransom or destroyed, …  *Als Folge dessen können Sie von Ihrem eigenen PC ausgesperrt sein, Ihre Daten können zerstört oder für Lösegeldforderungen gestohlen werden, ...* | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … your core computer components can be seized for malicious purposes, or you may be spied on.  *… wesentliche Komponenten Ihres Computers können für böswillige Zwecke missbraucht werden oder Sie werden ausspioniert.* | 1. PC in the middle 2. Its components around it 3. Warning icons pops up over each component 4. Everything slides to the left and a tap appears 5. Data flow out of the PC towards the hacker |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from?  *Das klingt tatsächlich sehr bösartig, oder nicht?*  *Aber woher kommt Malware?* | 1. Old PC appears 2. Floppy disk appears and it gets a malware 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was at its primitive stage and could only spread via physical means, …  *In den 1970er- und 80er-Jahren war Malware noch auf einem primitiven Level und konnte nur auf physikalischem Wege übertragen werden, …* | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another.  *… wie z. B. über Disketten, die manuell von einem Computer auf einen anderen eingelegt werden mussten.* | 1. A floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | Nowadays, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices in no time.  *Heutzutage jedoch breitet sich Malware mit der enormen Leistung des Internets virtuell aus und kann in wenigen Sekunden Tausende von Geräten infizieren.* | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor is at risk.  *Alles, was einen Mikroprozessor hat, ist gefährdet.* | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more.  *Dies schließt alle „intelligenten“ Geräte wie Uhren, Glühbirnen, Heizungen, Fahrzeuge und vieles mehr ein.* | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by a malware.  *Laut einer Statistik wurden bereits mehr als ein Drittel aller Computer dieser Welt einmal mit Malware infiziert.* | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and Trojans.  Let’s explore them in brief.  *Es gibt viele Arten von Malware und Sie haben wahrscheinlich schon von Viren, Ransomware, Würmern und Trojanern gehört.*  *Sehen wir uns das einmal genauer an.* | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years.  *Ransomware wurde in den letzten Jahren bei Hackern immer beliebter.* | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files.  *Üblicherweise wird der Zugriff auf Ihr System blockiert und gleichzeitig Ihre Dateien verschlüsselt.* | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of making public your private life, which may be embarrassing. Getting you to pay a ransom is the goal of this type of malware.  *Womöglich erhalten Sie sogar die Drohung, Ihr Privatleben öffentlich zu machen, was mitunter peinlich sein kann. Diese Art von Malware verfolgt das Ziel, Sie zur Zahlung eines Lösegelds zu bewegen.* | 1. The previous message disappears 2. The info icon pops up instead 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge.  *Spyware infiziert Ihre Geräte mit dem Zweck, an persönliche oder geschäftliche Informationen zu gelangen - ohne Ihr Wissen und Ihre Erlaubnis.* | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing is an example.  *Ein Beispiel sind Tracking-Cookies, die Ihr Surfverhalten im Internet überwachen.* | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package.  *Spyware gelangt normalerweise auf verdeckte Weise in ein System, z. B. durch Klicken auf ein Icon in einem Popup-Fenster oder durch Installieren eines größeren Softwarepakets.* | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you really know what it is?  *Die meisten Benutzer haben schon von Computerviren gehört. Aber wissen Sie darüber wirklich Bescheid?* | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | A virus is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems.  *Ein Virus ist eine Art von Malware, die menschliche Interaktion benötigt und ausgeführt werden muss, um andere Dateien zu infizieren oder auf andere Programme oder Systeme übertragen zu werden.* | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today.  *Aufgrund dieses Sachverhalts sehen wir heute reine Computerviren eher selten.* | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are Trojans, which pretend to be legitimate programs, but once installed - …  *Eine weitere bekannte Art von Malware sind Trojaner, die sich als legitime Programme ausgeben, aber wenn sie einmal installiert sind ...* | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system.  *… können Ihre Daten gestohlen, andere Malware installiert, Ihre Festplatte zerstört oder Ihr System auf andere Weise beschädigt werden.* | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware.  *Zum Glück gibt es Möglichkeiten, sich vor all diesen Formen von Malware zu schützen.* | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters.  *Zunächst, halten Sie Ihre Software auf dem letzten Stand. Ignorieren Sie niemals Systemaktualisierungen und -Upgrades und vergewissern Sie sich, dass Ihre Firewall, Antiviren- und Anti-Malware-Software, Ihr Browser und Spam-Filter in der neuesten Version sind.* | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well.  *Überprüfen Sie auch regelmäßig Ihre mobilen Geräte auf verfügbare Sicherheitsupdates.* | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method that can protect you from a potential breach, as hackers will have a hard time decrypting any encrypted information.  *Die Verschlüsselung Ihrer Dataien sind eine gute Methode, denn nach einem Angriff wird es für den Hacker schwierig, Ihre verschlüsselten Informationen zu entschlüsseln.* | 1. Laptop appears with different data files connected via cloud 2. Every file gets the lock icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent.  *Eine tägliche Sicherung Ihrer Daten ist dringend zu empfehlen und ein Datenträger in Form von Hardware ist in der Regel besser geschützt ist als eine Cloud-Alternative. Im Falle eines Ransomware-Angriffs können Sie auf Ihre Dateien zugreifen, ohne einen Cent zu bezahlen.* | 1. Continuation of the previous scene 2. The laptop remains 3. Other devices appear around it 4. Then the backup icon pops up 5. Arrows go to it from the devices |  |
| **34** | Whenever you think of installing new apps, do it from trusted sources like Google Play Store and Apple App Store.  *Wenn Sie eine neue App installieren möchten, verwenden Sie nur vertrauenswürdige Quellen wie den Google Play Store oder den Apple App Store.* | 1. Continuation of the previous scene 2. The phone zooms to the screen 3. It shows Google Play Store app and the shield icon pops up 4. Then the Apple App Store is shown and the same shield icon pops up |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise, you may be at risk and be infected by a malware.  *Stellen Sie sicher, dass Sie Dateien und Dokumente nur in einem sicheren Umfeld herunterladen.*  *Andernfalls könnten Sie Gefahr laufen, von Malware infiziert zu werden.* | 1. Screen splits 2. Two scenarios appear 3. Left part - secure download button appears 4. Cursor clicks the download button 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as:  *Der beste Weg, sich und Ihr Unternehmen vor Malware zu schützen, besteht darin, allgemeine Sicherheitsmaßnahmen zu kennen und umzusetzen, wie beispielsweise:* | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Macros unless required.  • Always scanning external drives prior to use.  *• Verwenden einzigartiger und sicherer Passwörter.*  *• Überprüfen Sie die Legitimität aller URLs, an die Sie weitergeleitet werden.*  *• Aktivieren Sie niemals Makros, wenn dies nicht erforderlich ist.*  *• Scannen Sie externe Laufwerke immer vor deren Verwendung.* | 1. Computer with login page is shown 2. Password field appears and field shows that it is strong 3. Browser pops up and gets checked with a magnifying glass 4. Macros appears and the bar with a button is crossed out 5. Devices appear and get checked |  |
| **38** | Using your common sense can save you from most malware attacks.  *Wenn Sie Ihren gesunden Menschenverstand einsetzen, können Sie sich vor den meisten Malware-Angriffen schützen.* | 1. A head with spinning cogs appears 2. Data icon with a magnifying glass, a server with a lock and the encrypted document pop up 1 by 1 |  |
| **39** | In truth, your company’s network filters already block the majority of malware. Still, staying vigilant will not let the bad guys in no matter what new sophisticated method they use.  *In Wahrheit blockieren die Netzwerkfilter Ihres Unternehmens bereits den größten Teil der Malware. Dennoch heißt es, wachsam bleiben und das Böse nicht hereinlassen, egal welche neuen, raffinierten Methoden verwendet werden.* | 1. A network with firewall is shown 2. The hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks!  *Denken Sie daran, dass schlussendlich Sie die letzte und wichtigste Instanz gegen Malware-Angriffe sind!* | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo and text animation   www.lucysecurity.com |  |

**Lucy Malware Storyboard 4.0 (final design)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference:** [**GoodTime**](https://docs.google.com/document/d/1mVn6Vsg6I0f9m6mltLz3YjRdh1kAJvtGHEHidHPUfjw/edit?usp=sharing)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | LUCY’s Malware Awareness Video | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, it is easy to come across malware. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb and goes into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. A lock pops up on the screen and gets unlocked 2. Then the lock is changed by the malware icon 3. Two other laptops appear to represent a network 4. Phone pops up |  |
| **4** | As a result, you may be blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … your core computer components can be seized for malicious purposes, or you may be spied on. | 1. PC in the middle 2. Its components around it 3. Warning icons pops up over each component 4. Everything slides to the left and a tap appears 5. Data flow out of the PC towards the hacker |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Old PC appears 2. Floppy disk appears and it gets a malware 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was at its primitive stage and could only spread via physical means, ... | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. A floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | Nowadays, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices in no time. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by a malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and Trojans.  Let’s explore them in brief. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of making public your private life, which may be embarrassing. Getting you to pay a ransom is the goal of this type of malware. | 1. The previous message disappears 2. The info icon pops up instead 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing is an example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you really know what it is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | A virus is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are Trojans, which pretend to be legitimate programs, but once installed - ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method that can protect you from a potential breach, as hackers will have a hard time decrypting any encrypted information. | 1. Laptop appears with different data files connected via cloud 2. Every file gets the lock icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The laptop remains 3. Other devices appear around it 4. Then the backup icon pops up 5. Arrows go to it from the devices |  |
| **34** | Whenever you think of installing new apps, do it from trusted sources like Google Play Store and Apple App Store. | 1. Continuation of the previous scene 2. The phone zooms to the screen 3. It shows Google Play Store app and the shield icon pops up 4. Then the Apple App Store is shown and the same shield icon pops up |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise, you may be at risk and be infected by a malware. | 1. Screen splits 2. Two scenarios appear 3. Left part - secure download button appears 4. Cursor clicks the download button 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Macros unless required.  • Always scanning external drives prior to use. | 1. Computer with login page is shown 2. Password field appears and field shows that it is strong 3. Browser pops up and gets checked with a magnifying glass 4. Macros appears and the bar with a button is crossed out 5. Devices appear and get checked |  |
| **38** | Using your common sense can save you from most malware attacks. | 1. A head with spinning cogs appears 2. Data icon with a magnifying glass, a server with a lock and the encrypted document pop up 1 by 1 |  |
| **39** | In truth, your company’s network filters already block the majority of malware. Still, staying vigilant will not let the bad guys in no matter what new sophisticated method they use. | 1. A network with firewall is shown 2. The hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo and text animation   www.lucysecurity.com |  |

**Lucy Malware Storyboard 3.2 (drafts of design)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference:** [**GoodTime**](https://docs.google.com/document/d/1mVn6Vsg6I0f9m6mltLz3YjRdh1kAJvtGHEHidHPUfjw/edit?usp=sharing)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, it is easy to come across malware. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb and does into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. Computer screen appears 2. A lock pops up and gets unlocked 3. Then the lock is changed by the malware icon 4. Two other PC screens appear to represent a network 5. Phone pops up |  |
| **4** | As a result, you may be blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … your core computer components can be seized for malicious purposes, or you may be spied on. | 1. Pc in the middle 2. Its components around it 3. Malware icons pops up over each component 4. Tap |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Old PC appears 2. Floppy disk appears and it got a virus 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was at its primitive stage and could only spread via physical means, ... | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. a floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | Nowadays, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices in no time. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by a malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and Trojans.  Let’s explore them in brief. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of making public your private life, which may be embarrassing. Getting you to pay a ransom is the goal of this type of malware. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing is an example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you really know what it is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | A virus is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are Trojans, which pretend to be legitimate programs, but once installed - ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method tool that can protect you from a potential breach, as hackers will have a hard time decrypting any encrypted information. | 1. Computer appear with different data files connected via cloud 2. Every file get the icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **34** | Whenever you think of installing new apps, do it from trusted sources like Google Play Store and Apple App Store. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise, you may be at risk and be infected by a malware. | 1. Screen splits 2. Two scenarios appear 3. Left part - Secure download button appear 4. Button clicks the download 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Excel Macros unless required.  • Always scanning external drives prior to use. | 1. Computer with login page 2. Password field appears and field shows that it is strong 3. Browser pops up and get checked with magnifying glass 4. Macros appears and bar with button is crossed out 5. Devices appear and get checked |  |
| **38** | Using your common sense can save you from most malware attacks. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | In truth, your company’s network filters already block the majority of malware. Still, staying vigilant will not let in the bad guys no matter what new sophisticated method they use. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo and text animation animation   www.lucysecurity.com |  |

**Lucy Malware Storyboard 3.1 (drafts of design)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference:** [**GoodTime**](https://docs.google.com/document/d/1mVn6Vsg6I0f9m6mltLz3YjRdh1kAJvtGHEHidHPUfjw/edit?usp=sharing)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb and does into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. Computer screen appears 2. A lock pops up and gets unlocked 3. Then the lock is changed by the malware icon 4. Two other PC screens appear to represent a network 5. Phone pops up |  |
| **4** | As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … .. your core computer components can be kidnapped for malicious purposes, or you may get spied on. | 1. Pc in the middle 2. Its components around it 3. Malware icons pops up over each component 4. Tap |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Old PC appears 2. Floppy disk appears and it got a virus 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was primitive and could only spread via physical means, ... | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. a floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor in it is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.  Let’s explore them a little. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing are one such example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you know what a virus is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method tool that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information. | 1. Computer appear with different data files connected via cloud 2. Every file get the icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **34** | Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise you risk a malware infection. | 1. Screen splits 2. Two scenarios appear 3. Left part - Secure download button appear 4. Button clicks the download 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Excel Mmacros unless required.  • Always scanning external drives prior to use. | 1. Computer with login page 2. Password field appears and field shows that it is strong 3. Browser pops up and get checked with magnifying glass 4. Macros appears and bar with button is crossed out 5. Devices appear and get checked |  |
| **38** | Using your common sense can save you from most malware attacks. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo and text animation animation   www.lucysecurity.com |  |

**Lucy Malware Storyboard 3.0 (drafts of design)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference:** [**GoodTime**](https://docs.google.com/document/d/1mVn6Vsg6I0f9m6mltLz3YjRdh1kAJvtGHEHidHPUfjw/edit?usp=sharing)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb and does into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. Computer screen appears 2. A lock pops up and gets unlocked 3. Then the lock is changed by the malware icon 4. Two other PC screens appear to represent a network 5. Phone pops up |  |
| **4** | As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … .. your core computer components can be kidnapped for malicious purposes, or you may get spied on. | 1. Pc in the middle 2. Its components around it 3. Malware icons pops up over each component 4. Tap |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Old PC appears 2. Floppy disk appears and it got a virus 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was primitive and could only spread via physical means, ... | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. a floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row | **V1**    **V2**    **V3**    **V4** |
| **9** | In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor in it is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.  Let’s explore them a little. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing are one such example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you know what a virus is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method tool that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information. | 1. Computer appear with different data files connected via cloud 2. Every file get the icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place | **Bildergebnis für backup** |
| **34** | Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise you risk a malware infection. | 1. Screen splits 2. Two scenarios appear 3. Left part - Secure download button appear 4. Button clicks the download 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Excel Mmacros unless required.  • Always scanning external drives prior to use. | 1. Computer with login page 2. Password field appears and field shows that it is strong 3. Browser pops up and get checked with magnifying glass 4. Macros appears and bar with button is crossed out 5. Devices appear and get checked | **Bildergebnis für strong password** |
| **38** | Using your common sense can save you from most malware attacks. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo and text animation animation   www.lucysecurity.com |  |

**Lucy Malware Storyboard 2.3 (Scenario ideas)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference:** [**GoodTime**](https://docs.google.com/document/d/1mVn6Vsg6I0f9m6mltLz3YjRdh1kAJvtGHEHidHPUfjw/edit?usp=sharing)

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb and does into the computer screen 2. Death message pop up on the screen 3. More notifications of errors appear on the screen and around |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. Computer screen appears 2. A lock pops up and gets unlocked 3. Then the lock is changed by the malware icon 4. Two other PC screens appear to represent a network 5. Phone pops up |  |
| **4** | As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. The camera zooms to one of the screens 2. Padlock appears on the screen 3. Text animation under the lock requesting ransom 4. Hands appear with coins 5. Broken data icon appears on the screen |  |
| **5** | … .. your core computer components can be kidnapped for malicious purposes, or you may get spied on. | 1. Pc in the middle 2. Its components around it 3. Malware icons pops up over each component 4. Tap |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Old PC appears 2. Floppy disk appears and it got a virus 3. History data is animated |  |
| **7** | Back in the 1970s and 80s, malware was primitive and could only spread via physical means, ... | 1. Animation as in the example (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. a floppy disk zooms to the screen 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor in it is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.  Let’s explore them a little. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing are one such example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you know what a virus is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Computer screen receives notification 2. The button ‘accept’ is clicked 3. Zoom out and we see a worker at the computer while it is being updated |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Mobile phone appears with notification of updates |  |
| **32** | Data encryption is a method tool that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information. | 1. Computer appear with different data files connected via cloud 2. Every file get the icon |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place | **Bildergebnis für backup** |
| **34** | Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **35** | Make sure that you download files and documents only from places that are safe.  Otherwise you risk a malware infection. | 1. Screen splits 2. Two scenarios appear 3. Left part - Secure download button appear 4. Button clicks the download 5. Download process completes 6. Right part - website with lots of flashing ads animate 7. More ads and flashing arrows appear as scene progresses 8. Laptop on the right is crossed |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Network icon appears 2. Cloud of words appears in the background 3. Shield appears 4. Malware bounces off the shield |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling Excel Mmacros unless required.  • Always scanning external drives prior to use. | 1. Computer with login page 2. Password field appears and field shows that it is strong 3. Browser pops up and get checked with magnifying glass 4. Macros appears and bar with button is crossed out 5. Devices appear and get checked | **Bildergebnis für strong password** |
| **38** | Using your common sense can save you from most malware attacks. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **40** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **41** | NO VO | 1. Logo animation |  |

# **Lucy Malware Storyboard 2.2 (Scenario ideas)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference: Regular Lucy animation style mixed with this** [**Lucy video**](https://lucysecurity.com/wp-content/uploads/2019/01/social-engineering.mp4)

**We do not need real actors – but it is just all very simple and neutral**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it ... | 1. A spider goes down from the top of the screen on a cobweb 2. Text animation 3. “Malicious software” is shown as the VO mentions it   Can we show PC and how malware infects it? |  |
| **3** | … so they can gain access to or otherwise harm your computer system or network, or your mobile device. | 1. Computer screen appears 2. A lock pops up and gets unlocked 3. Then the lock is changed by the malware icon 4. Two other PC screens appear to represent a network 5. Phone pops up |  |
| **4** | As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, ... | 1. Icons are animated (kinda scrolled through) according to the VO   I dont like the animation; a bit simple / childish. Is the access denied on a PC? I think it needs something that visualizes this more clear |  |
| **5** | … .. your core computer components can be kidnapped for malicious purposes, or you may get spied on. | 1. Icons are animated (kinda scrolled through) according to the VO   I think the animation needs to relate to the topic and show pc with core components getting controlled by malware and at the same time informtion leakage from PC via malware to the hacker... |  |
| **6** | It does sound malicious, doesn’t it?  But where did malware come from? | 1. Text and icon animation according to the VO 2. Zoom in on the tablet screen as a transition to the next scene   Rather no text on screen → not necessary and needs to many adjustements when using different languages |  |
| **7** | Back in the 1970s and 80s, malware was primitive and could only spread via physical means, ... | 1. Text animation 2. The malware icon is shown 3. It turns into a more primitive one   The illustration is not clear: I dont see how a red bug is “older” than a green bug :-) I think it makes sense to show an animation of very old malware . Check out old animated gifs about virus (<https://www.google.com/search?q=animated+gif+old+pc+virus&source=lnms&tbm=isch&sa=X&ved=0ahUKEwi32MfsuabkAhWIbVAKHU8fCsoQ_AUIESgB&biw=1536&bih=754#imgrc=7TM9b_dWWjJ8OM:> |  |
| **8** | … like floppy disks that had to be manually carried from one computer to another. | 1. The “primitive” malware icon gets on a floppy disk 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **9** | In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes. | 1. Text animation 2. The Internet icon pops up, a magnifying glass is scrutinizing it 3. It finds malware there 4. Text animation according to the VO |  |
| **10** | Anything with a microprocessor in it is at risk. | 1. Zoom in on the malware icon 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **11** | This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **12** | According to statistics, over a third of the world’s computers have been infected by malware. | 1. Text animation 2. Numbers appear 3. The globe is shown 4. Numerous PCs pop up on it 5. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **13** | There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.  Let’s explore them a little. | 1. Icons and the corresponding text appear according to the VO |  |
| **14** | NO VO | 1. Text animation 2. Icon pops up |  |
| **15** | Ransomware gained much popularity in recent years. | 1. Continuation of the previous scene 2. A rising graph appears instead of the lock icon |  |
| **16** | Usually, it will block you from accessing your system, while also encrypting your files. | 1. A user in front of a PC is shown 2. “Access denied” pops up on the screen 3. The he gets an email and opens it 4. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **17** | You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates 4. Then a hand appears, it makes a gesture as if asking for money 5. A money bag falls into it |  |
| **18** | NO VO | 1. Text animation 2. Icon pops up |  |
| **19** | Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it 3. Docs pop up on the laptop 4. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **20** | Tracking cookies that monitor your web browsing are one such example. | 1. The icon appears on the laptop 2. Text animation |  |
| **21** | In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package. | 1. Some generic website is shown 2. Then the hacker from the previous scene appears half way in on the screen and adds the “Click here” text/a pop-up window 3. The window is being clicked 4. Icon for installation pops up |  |
| **22** | NO VO | 1. Text animation 2. Icon pops up |  |
| **23** | Most users have heard of computer viruses. But do you know what a virus is? | 1. Text remains from the previous scene but moves to the right 2. A user appears 3. A question mark pops up near the text |  |
| **24** | This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **25** | Because of this dependence, we rarely see pure computer viruses today. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **26** | NO VO | 1. Text animation 2. Icon pops up |  |
| **27** | Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **28** | … can destroy your hard drive, steal your data, install other malware, or otherwise harm your system. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **29** | Thankfully, there are ways to protect yourself from all these forms of malware. | 1. Text animation |  |
| **30** | First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters. | 1. Continuation of the previous scene 2. The text transforms into a new one 3. A list of tips is shown in a kind of banners 4. “Update your software” is being selected and zooms to the screen 5. Text animation according to the VO   We shopuld not have any text for the following slides. Lets visualize each topic. |  |
| **31** | Regularly check for available security updates on your mobile devices as well. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **32** | Data encryption is a method that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information. | 1. Continuation of the previous scene 2. Now the next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **33** | Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **34** | Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **35** | Make sure that you download files and documents only from places that are safe. Otherwise you risk a malware infection. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **36** | The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as: | 1. Continuation of the previous scene 2. The next banner is being selected |  |
| **37** | • Using unique and strong passwords.  • Checking the legitimacy of all URLs you are directed to.  • Never enabling acros unless required.  • Always scanning external drives prior to use. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place | **Bildergebnis für strong password** |
| **38** | Using your common sense can save you from most malware attacks. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
|  |  |  |  |
| **40** | In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **41** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **42** | NO VO | 1. Logo animation |  |

# **Lucy Malware Storyboard 2.1 (Scenario ideas)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference: Regular Lucy animation style mixed with this** [**Lucy video**](https://lucysecurity.com/wp-content/uploads/2019/01/social-engineering.mp4)

**We do not need real actors – but it is just all very simple and neutral**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | INTRO | 1. Logo and text animation |  |
| **3** | Malware, short for "malicious software," is any software that you don't want to have on your computer or mobile device. | 1. A spider goes down from the top of the screen on a cobweb 2. Text animation 3. Computer screen appears as a background 4. A hand drags a phone to the scene |  |
| **4** | It is a piece of software which is intended to cause harm to your system or network. | 1. The PC screen gets flooded with spiders |  |
| **5** | Malware has the ability to bring down the machine’s performance to knees, ... | 1. The screen turns blue and the alert pops up |  |
| **6** | … can cause a destruction of the network or system, steal, encrypt, or delete your data and also hijack core computer functions and finally spy on your computer activity without your knowledge or permission. | 1. The screen slides to the left 2. Text animation according to the VO |  |
| **7** | BRIEF HISTORY | 1. Logo and text animation |  |
| **8** | The earliest documented malware began to appear in the early 1970s. The term “virus” however, wasn’t introduced until the mid-eighties. | 1. The screen with malware is shown again 2. A hand with a magnifying glass appears scrutinizing it 3. Text animation 4. The first screen slides to the left and one more screen (with a virus icon) is shown on the right 5. The hand starts scrutinizing the latter 6. Text animation |  |
| **9** | Early malware was primitive, ... | 1. Zoom in on the malware icon from the previous scene 2. It turns into a more primitive one |  |
| **10** | … often spreading entirely offline via floppy disks carried from computer to computer by human hands. | 1. The “primitive” malware icon gets on a floppy disk 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **11** | As networking and the Internet matured, malware authors were quick to adapt their malicious code and take advantage of the new communication medium. | 1. One of the PC screens from the previous scene zooms in to the screen 2. The PC screen is shown with some random web search layout 3. Then a hacker appears, data processing at the background |  |
| **12** | Although malware gained much of its initial footing by infecting computers like PCs, today virtually anything with a microprocessor is at risk. | 1. Malware icon pops up 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **13** | Malware can infect hundreds of new targets, including wearables like watches, light bulbs, automobiles, water supply systems, and even airliners. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **14** | Today malware has infected one-third of the world’s computers. The consequences are staggering. | 1. Numbers appear 2. The globe is shown 3. Numerous PCs pop up on it 4. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **15** | MOST COMMON TYPES OF MALWARE | 1. Logo and text animation |  |
| **16** | Malware comes in many flavors. The most common types are virus, ransomware, worms, trojans, spyware and rootkits  We will dig into a few examples. | 1. Icons and the corresponding text appears according to the VO |  |
| **17** | **Ransomware** | 1. Text animation 2. Icon pops up |  |
| **18** | In recent years, ransomware has quickly become one of the most prevalent types of malware. | 1. The hand drags in a rising graph and puts it instead of the lock icon |  |
| **19** | The most common malware variants lock up a system, preventing any work from being done until the victim pays a ransom to the attacker. | 1. A user gets an email and opens it 2. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **20** | Other forms of ransomware threaten to publicize embarrassing information, such as a user's activity on adult websites, unless he or she pays a ransom. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates |  |
| **21** | **Spyware** | 1. Text animation 2. Icon pops up |  |
| **22** | Spyware is any type of software that gathers information about someone without their knowledge or consent. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it |  |
| **23** | For example, website tracking cookies that monitor a user's Web browsing can be considered a form of spyware. | 1. The icon appears on the laptop 2. Text animation |  |
| **24** | Other types of spyware might attempt to steal personal or corporate information. | 1. Continuation of the previous scene 2. Docs pop up on the laptop 3. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **25** | Spyware usually ends up on your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. | 1. Showing multiple generic program icons on the laptop screen 2. Then a pop-up window appears, it is being clicked 3. Two other icons are shown as the VO mentions them |  |
| **26** | **Virus** | 1. Text animation 2. Icon pops up |  |
| **27** | Sometimes people use the words "virus" and "malware" interchangeably, but a virus is actually a very specific kind of malware. | 1. Text animation 2. The hand wipes “Malware” away |  |
| **28** | In order to be considered a virus, the malware requires human intervention to run and propagate and must infect another program and attempt to spread itself to other systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **29** | Pure computer viruses are uncommon today, comprising less than 10 percent of all malware. Viruses are the only type of malware that "infects" other files. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **30** | **Trojan** | 1. Text animation 2. Icon pops up |  |
| **31** | A trojan presents itself as or hides in a legitimate program. For example, a Trojan might appear to be a free game, but once it is installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **32** | … it might destroy your hard drive, steal data, install a backdoor or take other harmful actions. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **33** | So how do you protect yourself from malware? | 1. Text animation |  |
| **34** | **Update your software**  Whenever your OS prompts you for an update, download it. Aside from the OS, update your browsers, antivirus software, anti-malware software, firewall, and spam filters. | 1. Continuation of the previous scene 2. The text goes to the top 3. A list of tips is shown in a kind of banners 4. “Update your software” is being selected and zooms to the screen 5. Text animation according to the VO |  |
| **35** | To protect against security flaws in mobile phones, be sure your mobile phone software is updated regularly. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **36** | **Encrypt your data**  Encrypting data is a defensive tool that can still protect your business in the event of a breach. Hackers would find sensitive data difficult to understand if it is encrypted. | 1. Continuation of the previous scene 2. Now the next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **37** | **Backup your data**  Backup your data often. Daily, if possible. Use hardware instead of cloud storage, as hackers can still access the latter. In the event of a ransomware attack, you would not have to pay to gain access to your files. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **38** | **Install only from trusted sources**  Install only from official or trusted sources like Google's Play Store and Apple's App Store. Apps can have malware inserted into them and still appear to work normally, so you will not always know if one is malicious. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | Avoid downloading files or documents from unfamiliar sources on your regular PC also as they might have some encrypted virus or other malware | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **40** | **Educate yourself**  You should be aware of security measures that every individual can take to help the company. | 1. Continuation of the previous scene 2. The next banner is being selected |  |
| **41** | Some of these include:  • Using unique and strong passwords.  • Paying attention to web page URLs and see if these are, for example, the legit website of a bank or an online store.  • Do not enable macro in excel if not required.  • Do not use any external drive without scanning. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **42** | **Common sense**  The easiest way to deal with malware is to not get it in the first place. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **43** | Experienced computer users avert potential disasters by practicing “skeptical computing,” which assumes that any new program is potentially harmful until proven safe. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **44** | The fact is that your company is already screening and filtering the majority of malware. However, the bad guys are always developing new tactics to get through to you. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **45** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **46** | NO VO | 1. Logo animation |  |

**Lucy Malware SCRIPT 1.1 (feel free to edit)**

This is LUCY’s Malware Awareness Video

In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it so they can gain access to or otherwise harm your computer system or network, or your mobile device.

As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, your core computer components may get hijacked for nefarious purposes, or you may get spied on.

It does sound malicious, doesn’t it?

But where did malware come from?

Back in the 1970s and 80s, malware was primitive and could only spread via physical means, like floppy disks that had to be manually carried from one computer to another.

In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes.

Anything with a microprocessor in it is at risk. This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more.

According to statistics, over a third of the world’s computers have been infected by malware.

There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.

Let’s explore them a little.

Ransomware gained much popularity in recent years. Usually, it will block you from accessing your system, while also encrypting your files. You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware.

Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. Tracking cookies that monitor your web browsing are one such example. In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package.

Most users have heard of computer viruses. But do you know what a virus is?

This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. Because of this dependence, we rarely see pure computer viruses today.

Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed can destroy your hard drive, steal your data, install other malware, or otherwise harm your system.

Thankfully, there are ways to protect yourself from all these forms of malware.

First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters.

Regularly check for available security updates on your mobile devices as well.

Data encryption is a tool that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information.

Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent.

Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. Make sure that you download files and documents only from places that are safe. Otherwise you risk a malware infection.

The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as:

• Using unique and strong passwords.

• Checking the legitimacy of all URLs you are directed to.

• Never enabling excel macros unless required.

• Always scanning external drives prior to use.

Using your common sense can save you from most malware attacks. So, make sure you don’t trust new programs until you see they are safe.

In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use.

Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks!

**Lucy Malware SCRIPT 1.0 (rough draft)**

This is LUCY’s Malware Awareness Video

In today’s digital world, malware is everywhere. But what is malware, exactly? Short for malicious software, hackers invented it so they can gain access to or otherwise harm your computer system or network, or your mobile device.

As a result, you may get blocked out of your own PC, your data may be stolen for ransom or destroyed, your core computer components may get hijacked for nefarious purposes, or you may get spied on.

It does sound malicious, doesn’t it?

But where did malware come from?

Back in the 1970s and 80s, malware was primitive and could only spread via physical means, like floppy disks that had to be manually carried from one computer to another.

In our days, however, with the huge power of the Internet, malware spreads virtually and can infect thousands of devices for mere minutes.

Anything with a microprocessor in it is at risk. This includes any “smart” devices, such as watches, light bulbs, heaters, automobiles, and many more.

According to statistics, over a third of the world’s computers have been infected by malware.

There are many types of malware, and you’ve most likely heard of viruses, ransomware, worms and trojans.

Let’s explore them a little.

Ransomware gained much popularity in recent years. Usually, it will block you from accessing your system, while also encrypting your files. You may even receive threats of your embarrassing private life going public. Getting you to pay a ransom is the goal of this type of malware.

Spyware infects your devices with the purpose of gathering personal or corporate information – without your permission or knowledge. Tracking cookies that monitor your web browsing are one such example. In any case, spyware usually enters a system by covert means, like clicking a button on a pop-up window or installing a larger software package.

Most users have heard of computer viruses. But do you know what a virus is?

This is a type of malware which infects other files and needs human interaction in order to run and spread to other programs or systems. Because of this dependence, we rarely see pure computer viruses today.

Another well-known type of malware are trojans, which pretend to be legitimate programs, but once installed can destroy your hard drive, steal your data, install other malware, or otherwise harm your system.

Thankfully, there are ways to protect yourself from all these forms of malware.

First, keep your software up-to-date. Never ignore system updates and upgrades, and always make sure you have the latest versions of your antivirus and anti-malware software, browsers, firewall, and spam filters.

Regularly check for available security updates on your mobile devices as well.

Data encryption is a tool that can protect you from a potential breach as hackers will have a hard time understanding any encrypted information.

Daily data backup is highly recommended, a hardware carrier usually being better protected than its cloud alternative. In case of a ransomware attack, you will be able to access your files without paying a cent.

Whenever you think of installing new apps, do it from trusted sources like the Google Play Store and the Apple App Store. Make sure that you download files and documents only from places that are safe. Otherwise you risk a malware infection.

The best way to protect yourself and your company from malware is to be aware of and implement common security measures, such as:

• Using unique and strong passwords.

• Checking the legitimacy of all URLs you are directed to.

• Never enabling excel macros unless required.

• Always scanning external drives prior to use.

Using your common sense can save you from most malware attacks. So, make sure you don’t trust new programs until you see they are safe.

In truth, the majority of malware is already picked up by your company’s network filters. Still, staying vigilant will not let in the bad guys no matter what new sophisticated scheme they use.

Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks!

**Lucy Malware Storyboard 2.0 (PLEASE IGNORE THIS VERSION)**

**Website and color combination:** [**https://lucysecurity.com**](https://lucysecurity.com)

**video reference: Regular Lucy animation style mixed with this** [**Lucy video**](https://lucysecurity.com/wp-content/uploads/2019/01/social-engineering.mp4)

**We do not need real actors – but it is just all very simple and neutral**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Voice-over** | **Action Plan** | **Storyboard** |
| **1** | This is LUCY’s Malware Awareness Video. | 1. Logo animation 2. A woman sitting in front of a laptop is shown |  |
| **2** | INTRO | 1. Logo and text animation |  |
| **3** | Malware, short for "malicious software," is any software that you don't want to have on your computer or mobile device. | 1. A spider goes down from the top of the screen on a cobweb 2. Text animation 3. Computer screen appears as a background 4. A hand drags a phone to the scene |  |
| **4** | It is a piece of software which is intended to cause harm to your system or network. | 1. The PC screen gets flooded with spiders |  |
| **5** | Malware has the ability to bring down the machine’s performance to knees, ... | 1. The screen turns blue and the alert pops up |  |
| **6** | … can cause a destruction of the network or system, steal, encrypt, or delete your data and also hijack core computer functions and finally spy on your computer activity without your knowledge or permission. | 1. The screen slides to the left 2. Text animation according to the VO |  |
| **7** | BRIEF HISTORY | 1. Logo and text animation |  |
| **8** | The earliest documented malware began to appear in the early 1970s. The term “virus” however, wasn’t introduced until the mid-eighties. | 1. The screen with malware is shown again 2. A hand with a magnifying glass appears scrutinizing it 3. Text animation 4. The first screen slides to the left and one more screen (with a virus icon) is shown on the right 5. The hand starts scrutinizing the latter 6. Text animation |  |
| **9** | Early malware was primitive, ... | 1. Zoom in on the malware icon from the previous scene 2. It turns into a more primitive one |  |
| **10** | … often spreading entirely offline via floppy disks carried from computer to computer by human hands. | 1. The “primitive” malware icon gets on a floppy disk 2. Zoom out and show it in the hand of a hacker 3. A computer appears at the background 4. Another person is shown and the hacker passes the floppy disk to him 5. More computers pop up at the background and move to the left in a single row |  |
| **11** | As networking and the Internet matured, malware authors were quick to adapt their malicious code and take advantage of the new communication medium. | 1. One of the PC screens from the previous scene zooms in to the screen 2. The PC screen is shown with some random web search layout 3. Then a hacker appears, data processing at the background |  |
| **12** | Although malware gained much of its initial footing by infecting computers like PCs, today virtually anything with a microprocessor is at risk. | 1. Malware icon pops up 2. PC is shown 3. Then other icons pop up 1 by 1 |  |
| **13** | Malware can infect hundreds of new targets, including wearables like watches, light bulbs, automobiles, water supply systems, and even airliners. | 1. Continuation of the previous scene 2. Icons appear as the VO mentions them |  |
| **14** | Today malware has infected one-third of the world’s computers. The consequences are staggering. | 1. Numbers appear 2. The globe is shown 3. Numerous PCs pop up on it 4. Zoom in on everything in the scene for kind of a dramatic effect |  |
| **15** | MOST COMMON TYPES OF MALWARE | 1. Logo and text animation |  |
| **16** | Malware comes in many flavors. The most common types are virus, ransomware, worms, trojans, spyware and rootkits  We will dig into a few examples. | 1. Icons and the corresponding text appears according to the VO |  |
| **17** | **Ransomware** | 1. Text animation 2. Icon pops up |  |
| **18** | In recent years, ransomware has quickly become one of the most prevalent types of malware. | 1. The hand drags in a rising graph and puts it instead of the lock icon |  |
| **19** | The most common malware variants lock up a system, preventing any work from being done until the victim pays a ransom to the attacker. | 1. A user gets an email and opens it 2. Showing the contents of the message (an example how ransomware encrypts files and asks for ransom) |  |
| **20** | Other forms of ransomware threaten to publicize embarrassing information, such as a user's activity on adult websites, unless he or she pays a ransom. | 1. The user closes the previous message 2. The info icon pops up 3. It pulsates |  |
| **21** | **Spyware** | 1. Text animation 2. Icon pops up |  |
| **22** | Spyware is any type of software that gathers information about someone without their knowledge or consent. | 1. A laptop with some info, e.g. a password, is shown 2. Binoculars appear watching at it |  |
| **23** | For example, website tracking cookies that monitor a user's Web browsing can be considered a form of spyware. | 1. The icon appears on the laptop 2. Text animation |  |
| **24** | Other types of spyware might attempt to steal personal or corporate information. | 1. Continuation of the previous scene 2. Docs pop up on the laptop 3. A hacker (symbolizing spyware) is sneaking to steal info from the docs |  |
| **25** | Spyware usually ends up on your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. | 1. Showing multiple generic program icons on the laptop screen 2. Then a pop-up window appears, it is being clicked 3. Two other icons are shown as the VO mentions them |  |
| **26** | **Virus** | 1. Text animation 2. Icon pops up |  |
| **27** | Sometimes people use the words "virus" and "malware" interchangeably, but a virus is actually a very specific kind of malware. | 1. Text animation 2. The hand wipes “Malware” away |  |
| **28** | In order to be considered a virus, the malware requires human intervention to run and propagate and must infect another program and attempt to spread itself to other systems. | 1. “Virus” gets into the rows of data on the PC screen 2. A hacker appears 3. Showing the screen with icons 4. At first one of the icons gets maybe a stamp “Virus”, and then their number grows |  |
| **29** | Pure computer viruses are uncommon today, comprising less than 10 percent of all malware. Viruses are the only type of malware that "infects" other files. | 1. Icon of a virus pops up 2. Typography animation 3. Zoom in on the icon 4. The virus “eats” a file |  |
| **30** | **Trojan** | 1. Text animation 2. Icon pops up |  |
| **31** | A trojan presents itself as or hides in a legitimate program. For example, a Trojan might appear to be a free game, but once it is installed ... | 1. A user is downloading a “legitimate” program 2. Then executes the file |  |
| **32** | … it might destroy your hard drive, steal data, install a backdoor or take other harmful actions. | 1. Continuation of the previous scene 2. Once executed, a Trojan icon slides out of it and spiders scatter around on the PC screen 3. Alerts from an antivirus/anti-malware software pop up |  |
| **33** | So how do you protect yourself from malware? | 1. Text animation |  |
| **34** | **Update your software**  Whenever your OS prompts you for an update, download it. Aside from the OS, update your browsers, antivirus software, anti-malware software, firewall, and spam filters. | 1. Continuation of the previous scene 2. The text goes to the top 3. A list of tips is shown in a kind of banners 4. “Update your software” is being selected and zooms to the screen 5. Text animation according to the VO |  |
| **35** | To protect against security flaws in mobile phones, be sure your mobile phone software is updated regularly. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **36** | **Encrypt your data**  Encrypting data is a defensive tool that can still protect your business in the event of a breach. Hackers would find sensitive data difficult to understand if it is encrypted. | 1. Continuation of the previous scene 2. Now the next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **37** | **Backup your data**  Backup your data often. Daily, if possible. Use hardware instead of cloud storage, as hackers can still access the latter. In the event of a ransomware attack, you would not have to pay to gain access to your files. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **38** | **Install only from trusted sources**  Install only from official or trusted sources like Google's Play Store and Apple's App Store. Apps can have malware inserted into them and still appear to work normally, so you will not always know if one is malicious. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **39** | Avoid downloading files or documents from unfamiliar sources on your regular PC also as they might have some encrypted virus or other malware | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **40** | **Educate yourself**  You should be aware of security measures that every individual can take to help the company. | 1. Continuation of the previous scene 2. The next banner is being selected |  |
| **41** | Some of these include:  • Using unique and strong passwords.  • Paying attention to web page URLs and see if these are, for example, the legit website of a bank or an online store.  • Do not enable macro in excel if not required.  • Do not use any external drive without scanning. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO 4. The banner returns to its place |  |
| **42** | **Common sense**  The easiest way to deal with malware is to not get it in the first place. | 1. Continuation of the previous scene 2. The next banner is being selected 3. Text animation according to the VO |  |
| **43** | Experienced computer users avert potential disasters by practicing “skeptical computing,” which assumes that any new program is potentially harmful until proven safe. | 1. Continuation of the previous scene 2. The last sentence in the list appears 3. The banner returns to its place |  |
| **44** | The fact is that your company is already screening and filtering the majority of malware. However, the bad guys are always developing new tactics to get through to you. | 1. A network with firewall is shown 2. A hacker appears spreading malware 3. Firewall filters out some of the mails labeled “Malware” 4. The others reach laptops |  |
| **45** | Keep in mind that in the end, you’re the last and most important layer of defense against malware attacks! | 1. Continuation of the previous scene 2. Some of the emails that firewall didn’t filter out are recognized as malware by users 3. These emails fly into the bins |  |
| **46** | NO VO | 1. Logo animation |  |