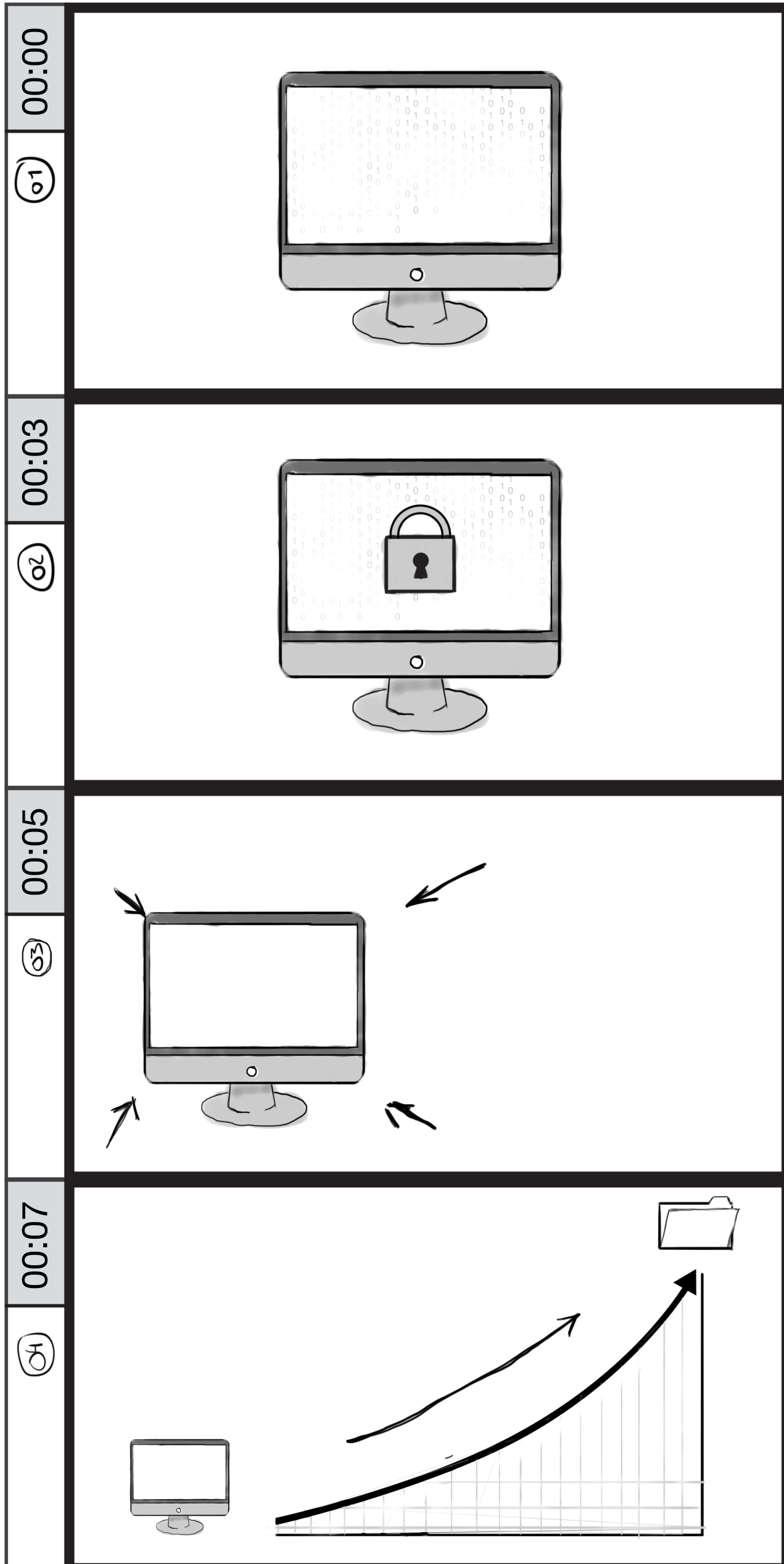


Title: Ransomware		Written By: Beth Burghardt
Director: Jeff Orloff	Storyboard: Joshua Rapp	Date: May 2016



NARRATOR:

Security incidents involving ransomware...

NARRATOR:

...are rapidly increasing.

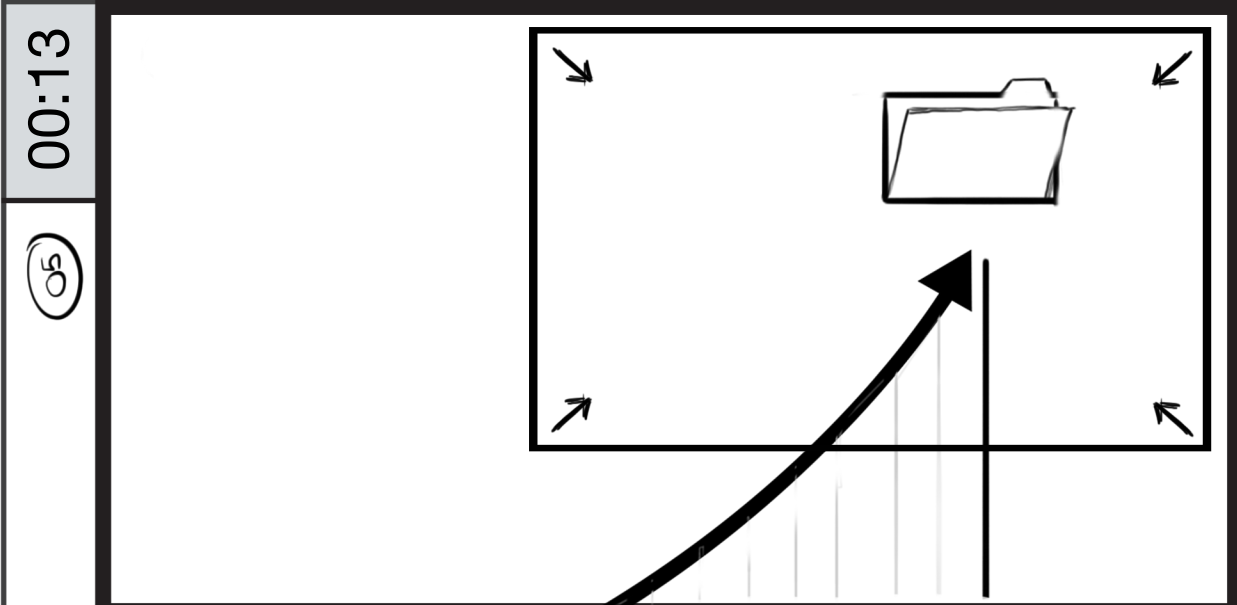
A lock appears on the screen in front of the falling binary code.

The computer screen shrinks down into the lower left portion of the shot.

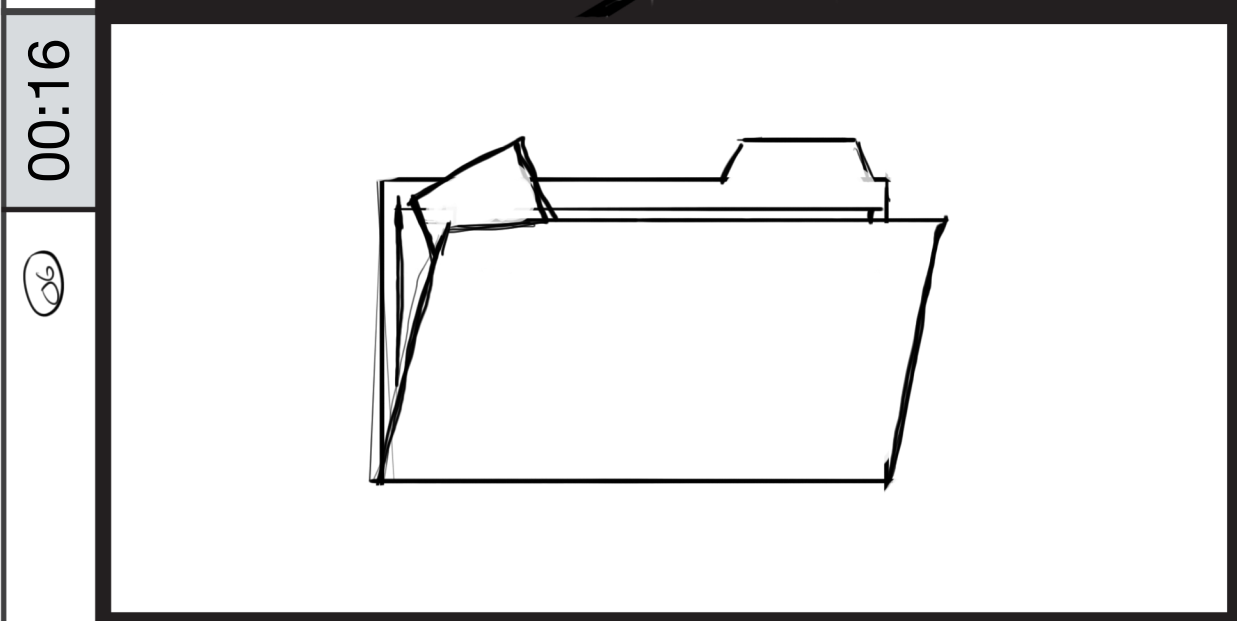
NARRATOR:

In 2015, over 750,000 computers were infected by ransomware.

A chart with a rising arrow animates upward from the left. Then a folder appears at the top of the chart.

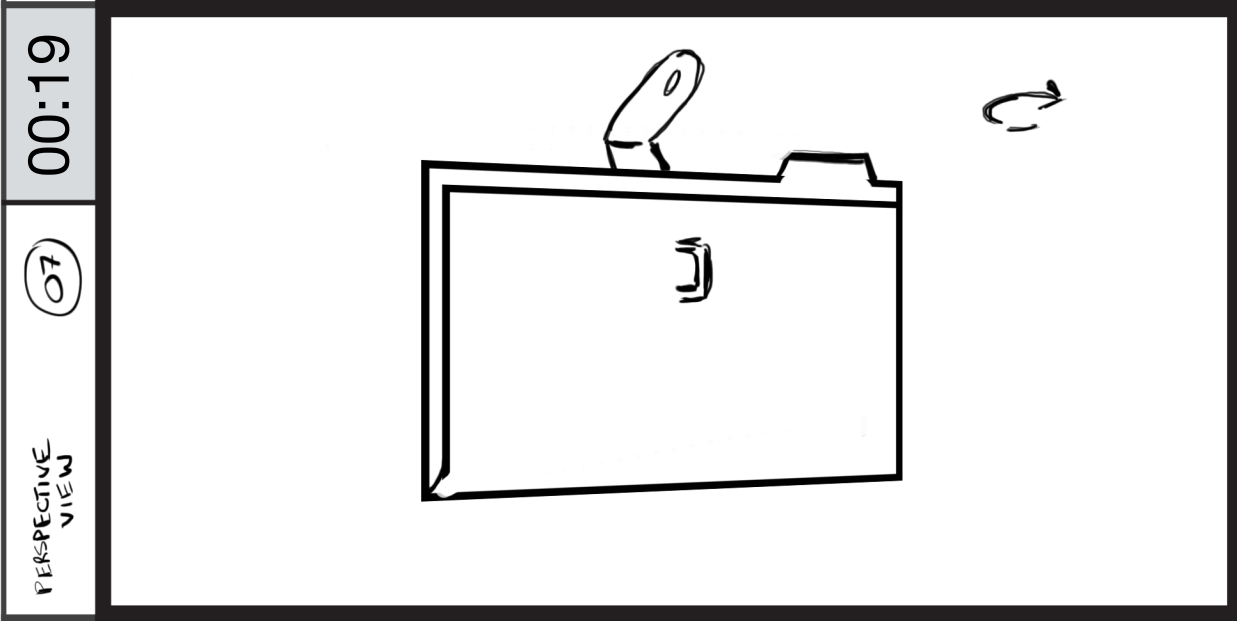


The camera zooms in placing focus on the folder.



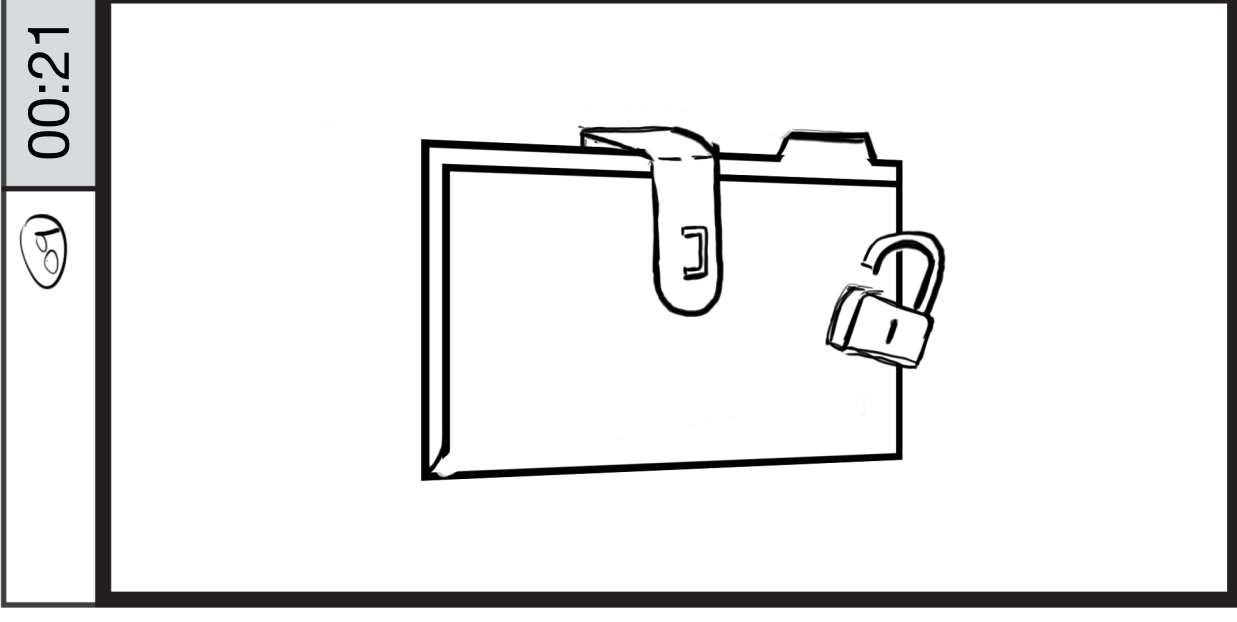
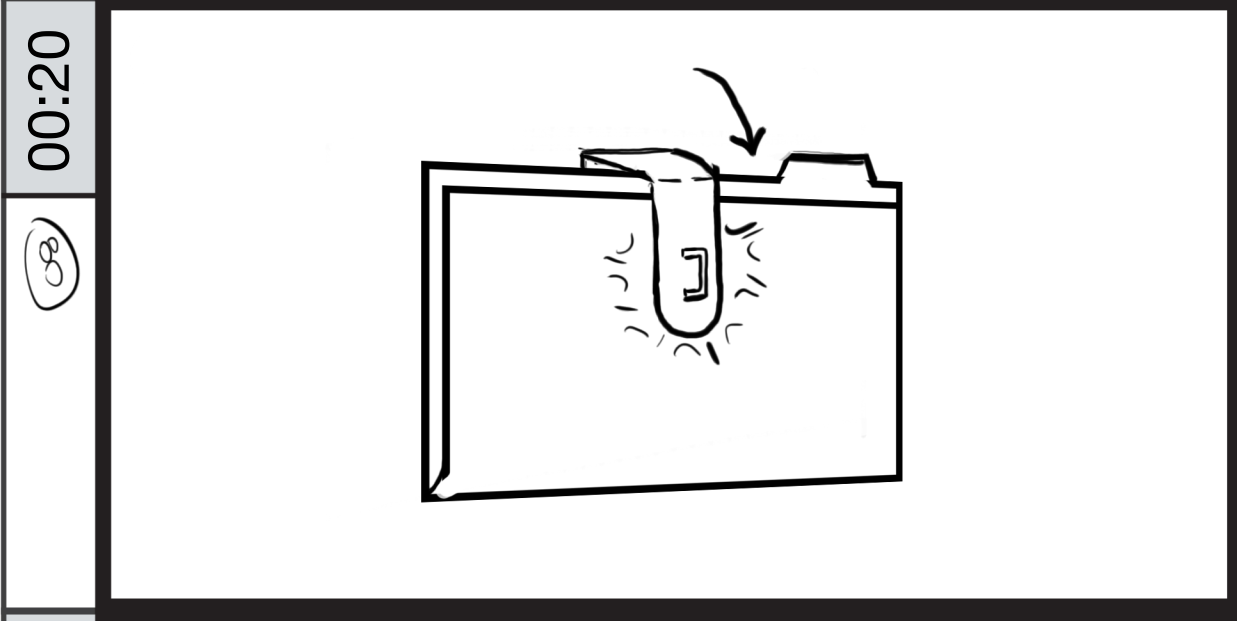
NARRATOR:
Ransomware is a type of malware that encrypts...

The folder centers in the shot and the chart fades away.



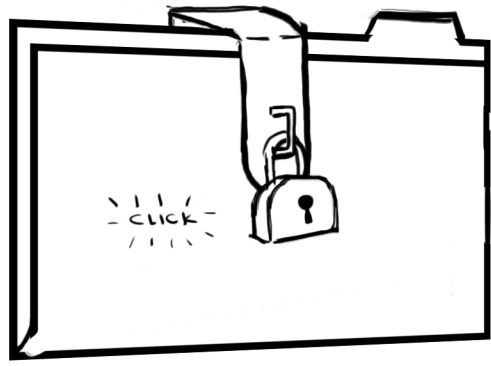
NARRATOR:
...or locks, computer files, making them nearly impossible to recover.

The folder turns slightly to the left and a latch appears from behind the folder.



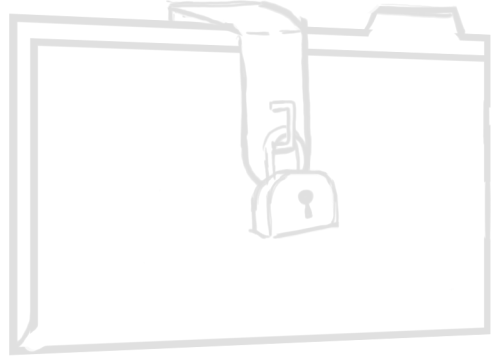
00:22

10



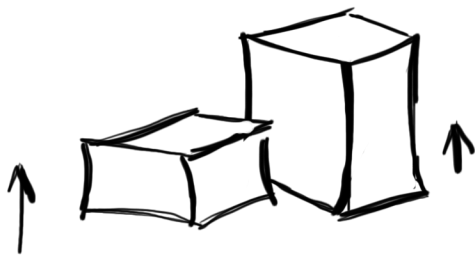
00:24

11



00:26

12



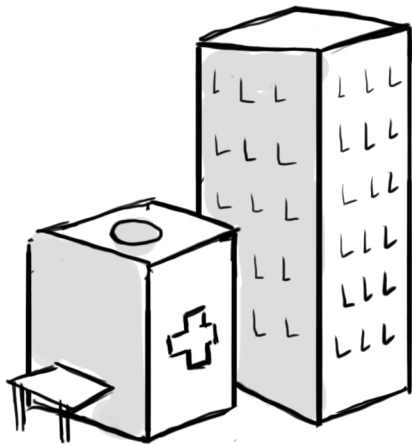
NARRATOR:

Large and small organizations are falling victim to ransomware attacks.

Two buildings grow up out of the ground with a bouncing ease-out, so there is a spring to the finished building.

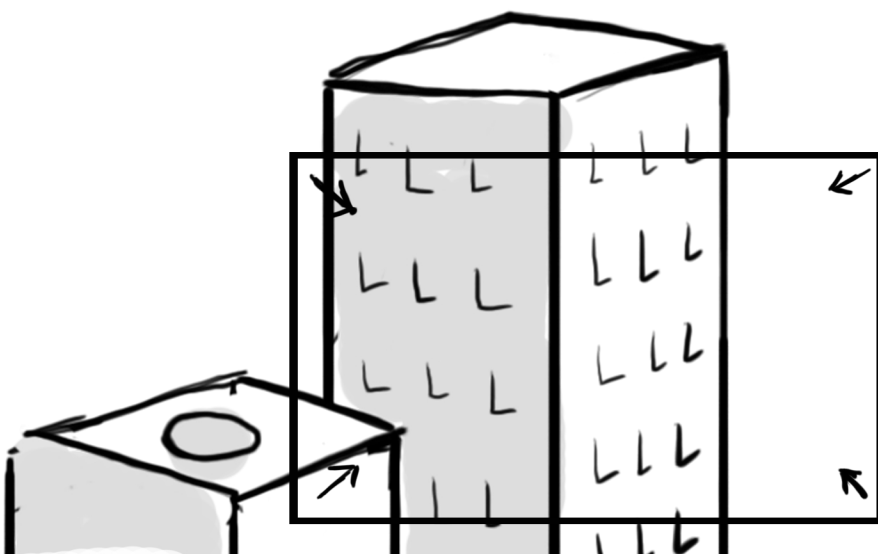
00:28

13



00:30

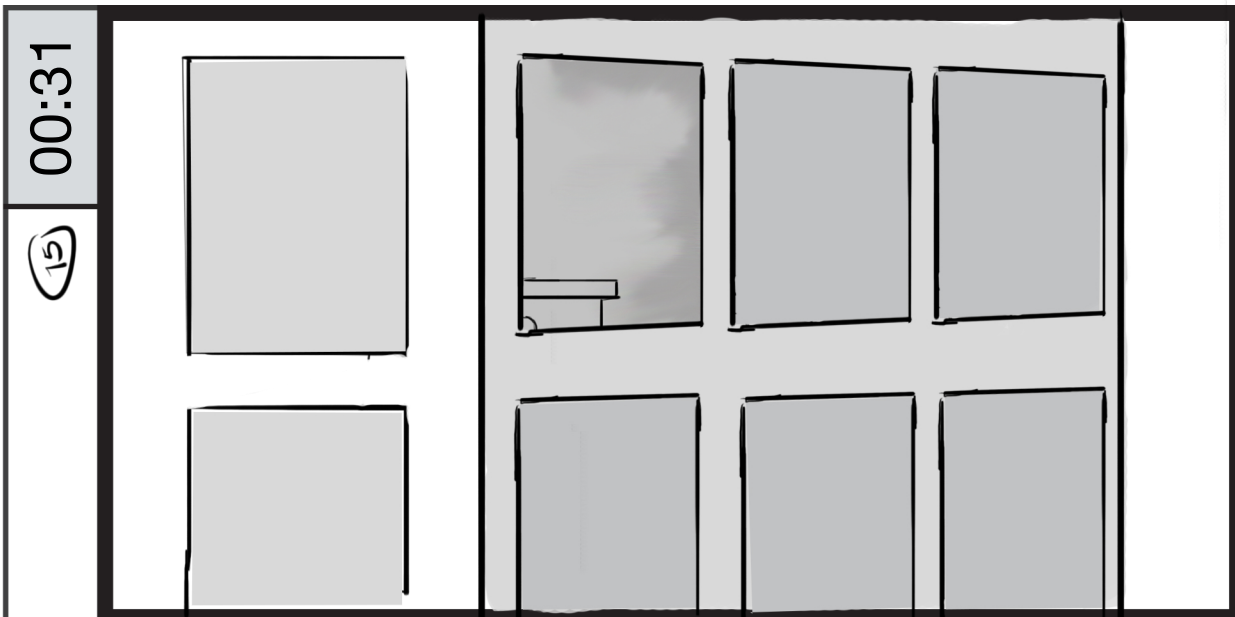
14



NARRATOR:

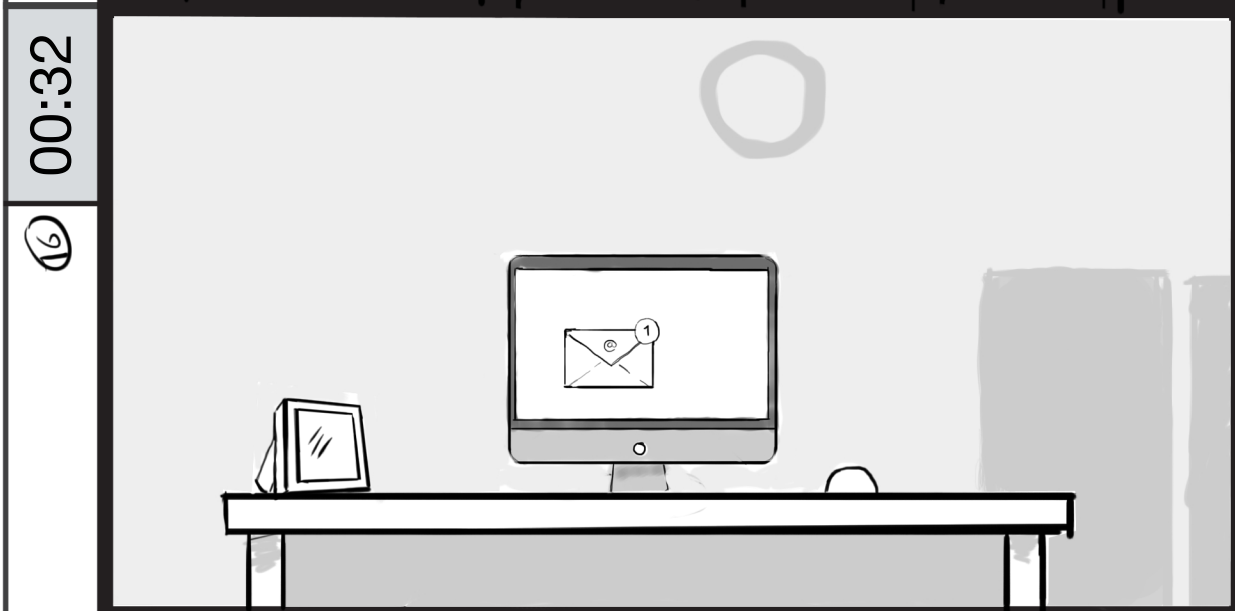
How does a ransomware attack happen?

The camera zooms into one of the office building windows to transition the shot.



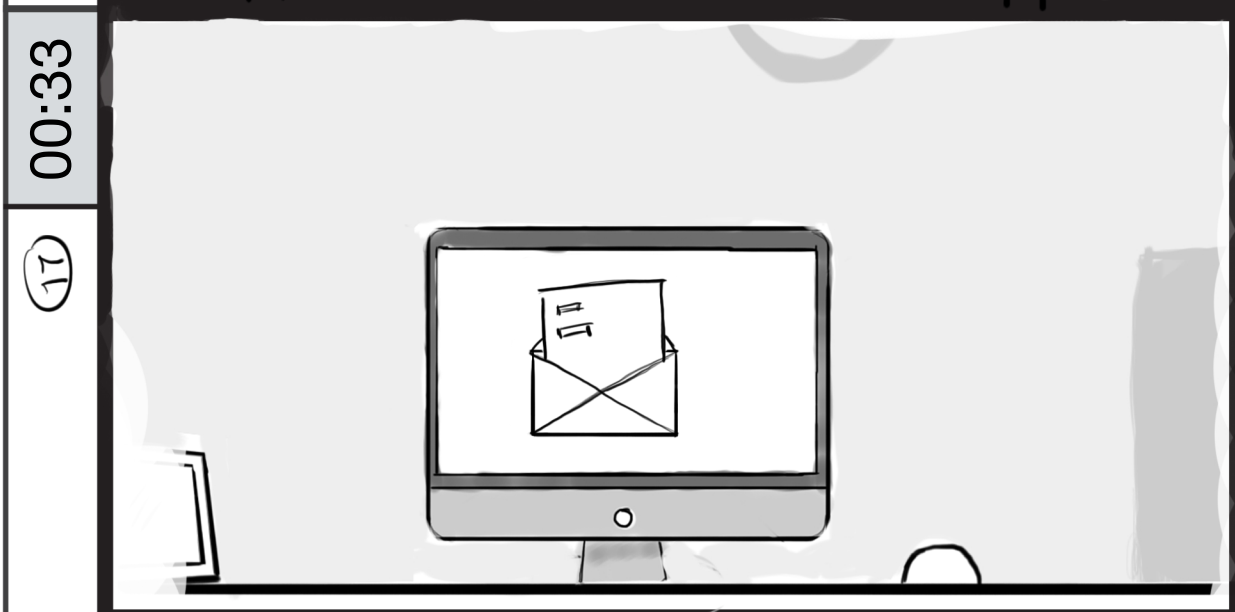
00:31

15



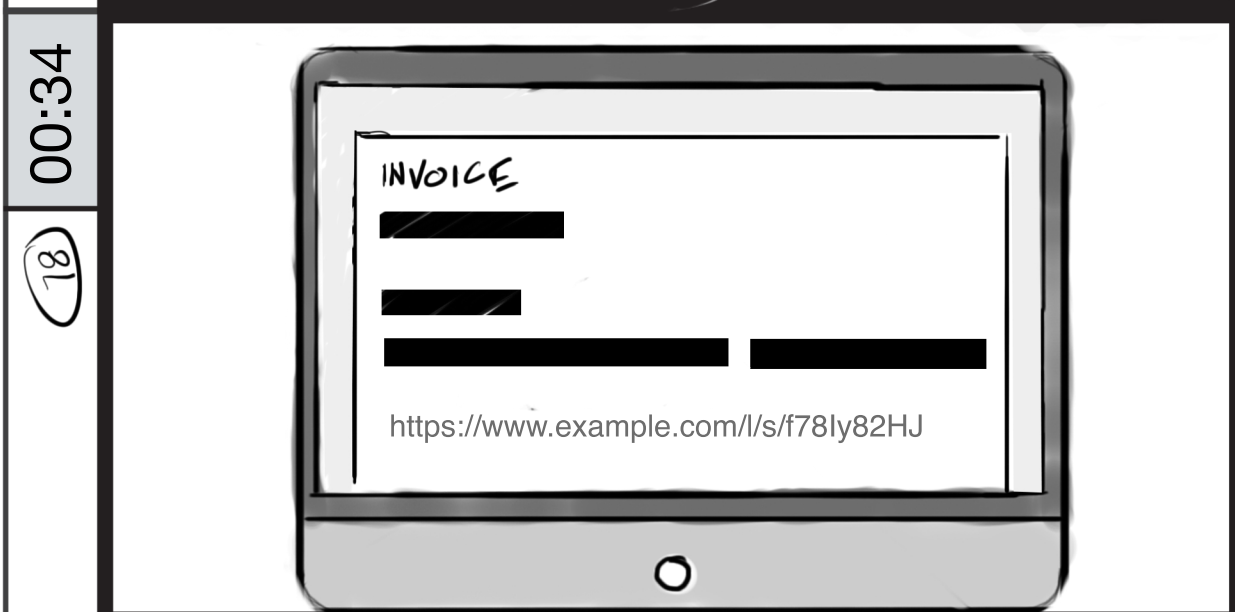
00:32

16



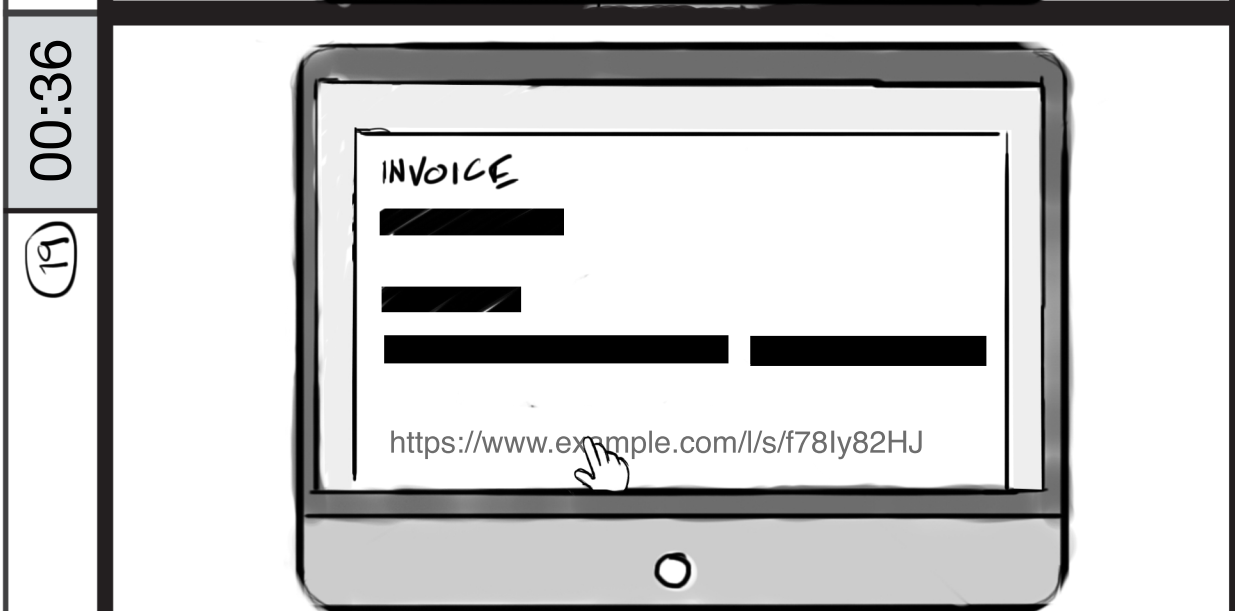
00:33

17



00:34

18



00:36

19

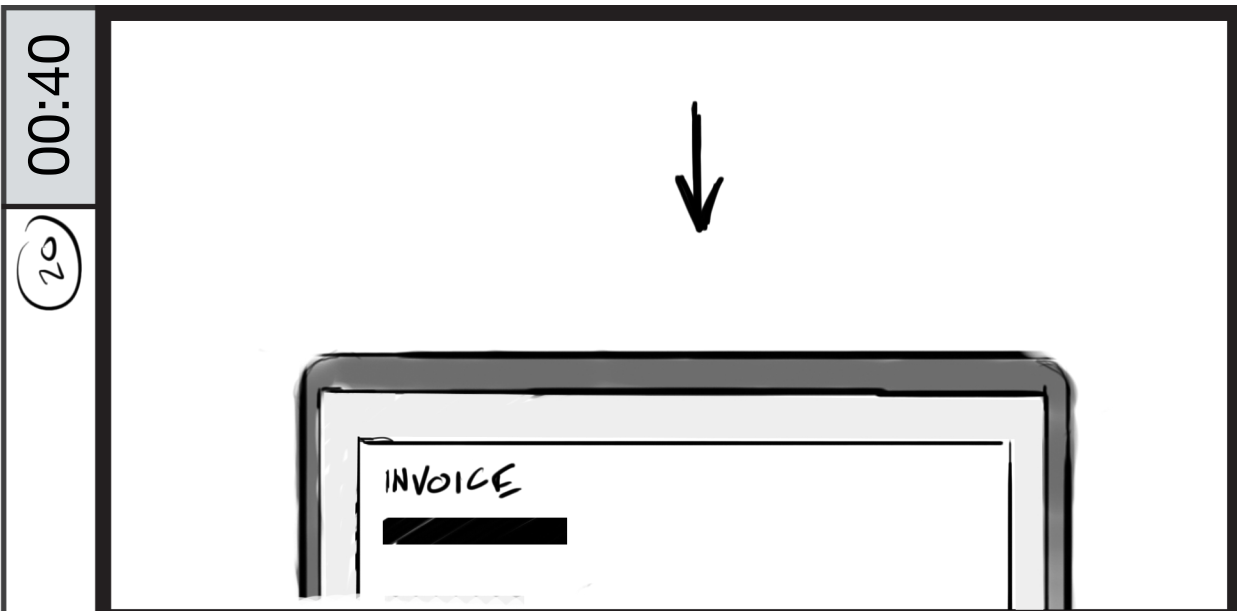
NARRATOR:

Ransomware is typically distributed in phishing emails.

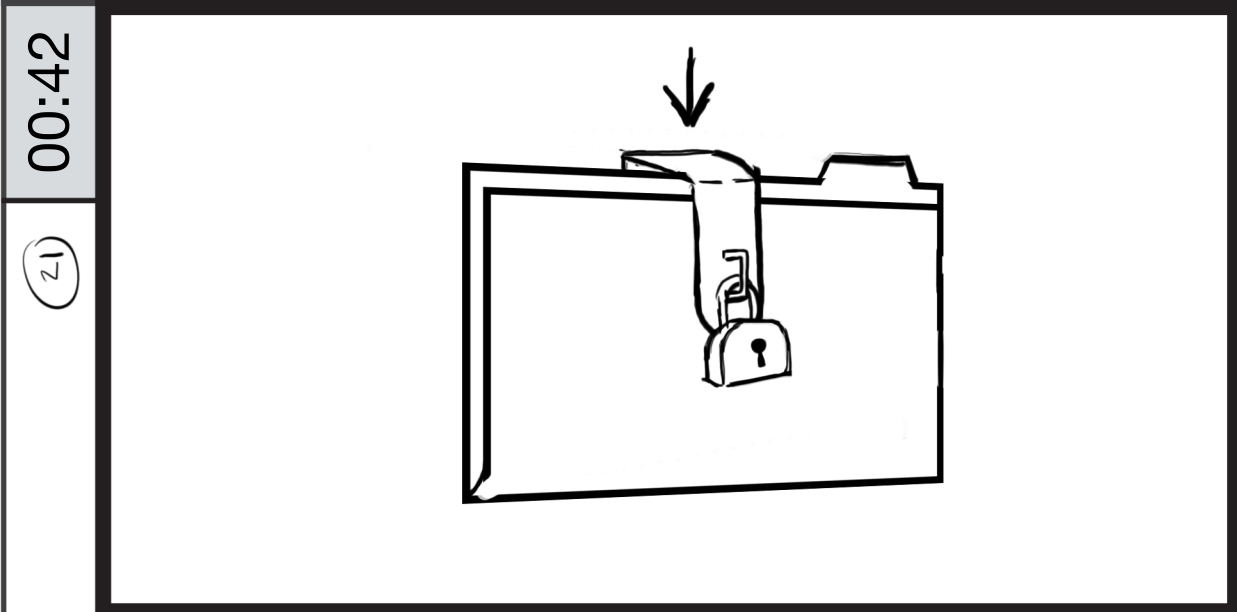
An email appears on the screen and the envelope begins to open.

NARRATOR:

Unaware of the scam, the recipient downloads a file attachment or clicks a malicious link.

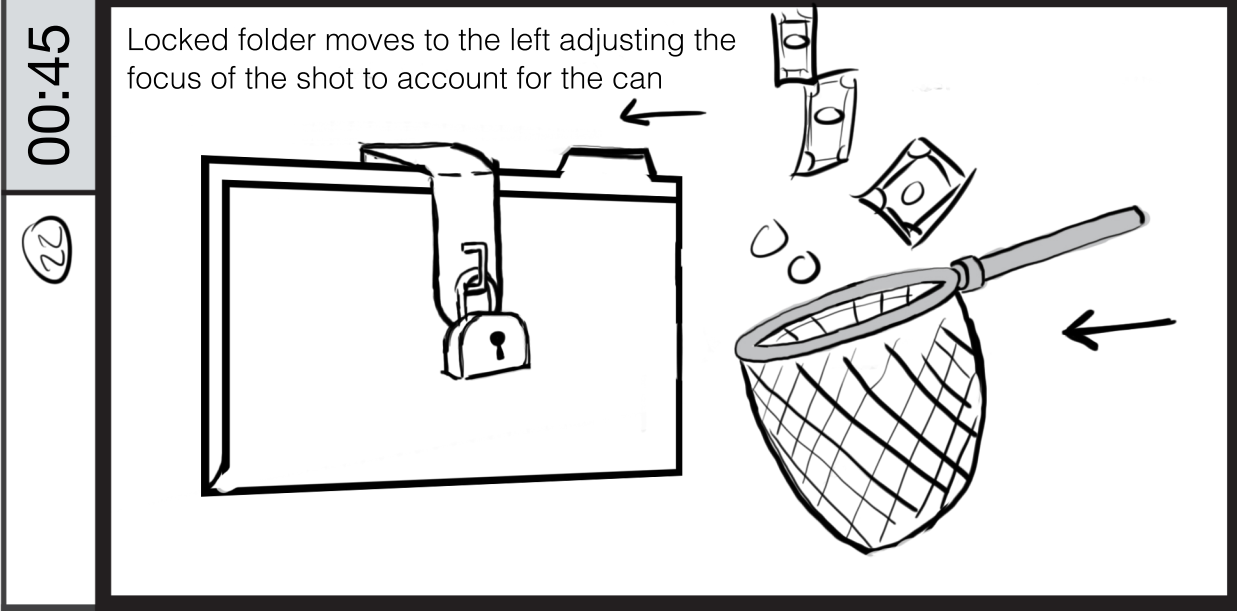


The monitor animates downward transitioning out of the shot.



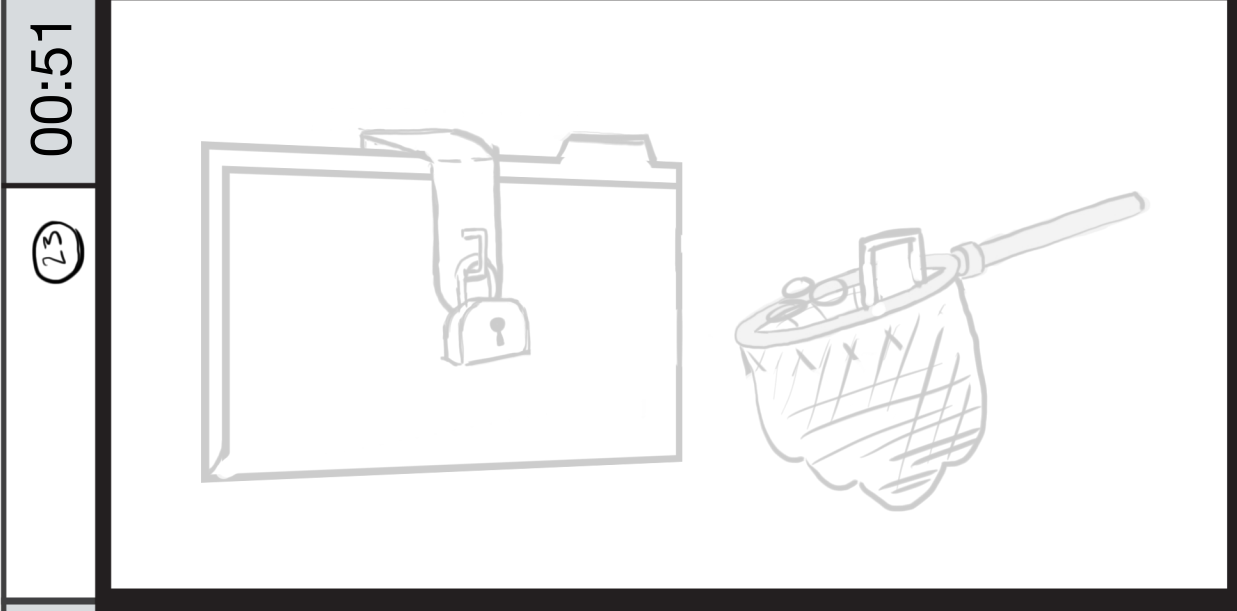
NARRATOR:

Once the computer is infected and files are encrypted...

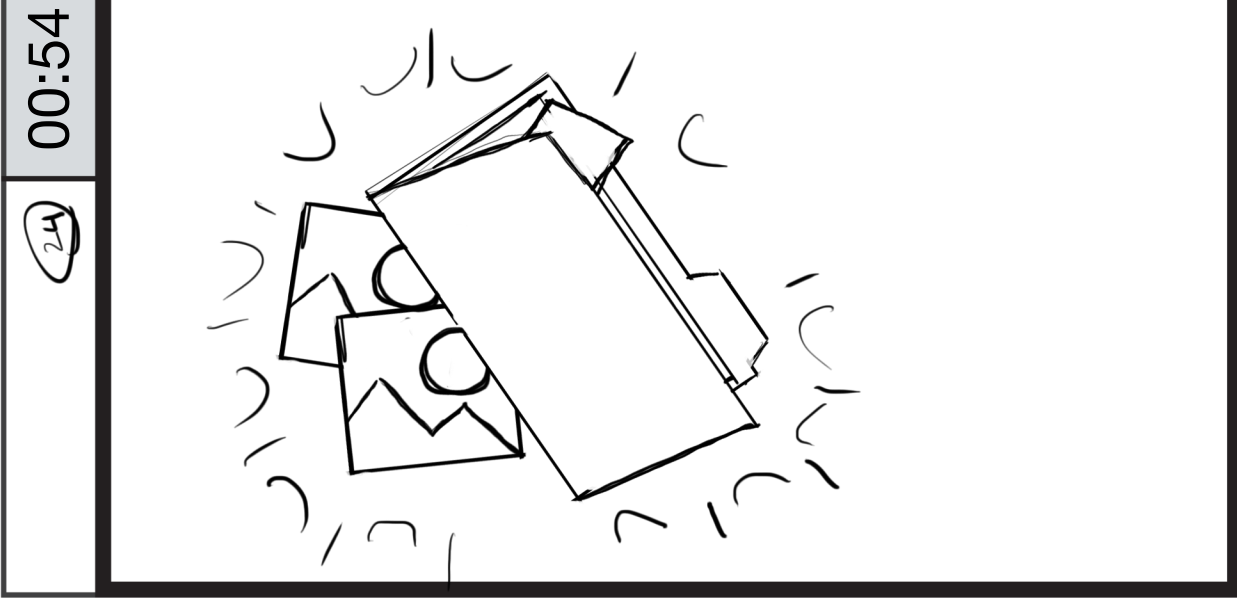


NARRATOR:

the attacker demands payment of a ransom in exchange for access to the files.

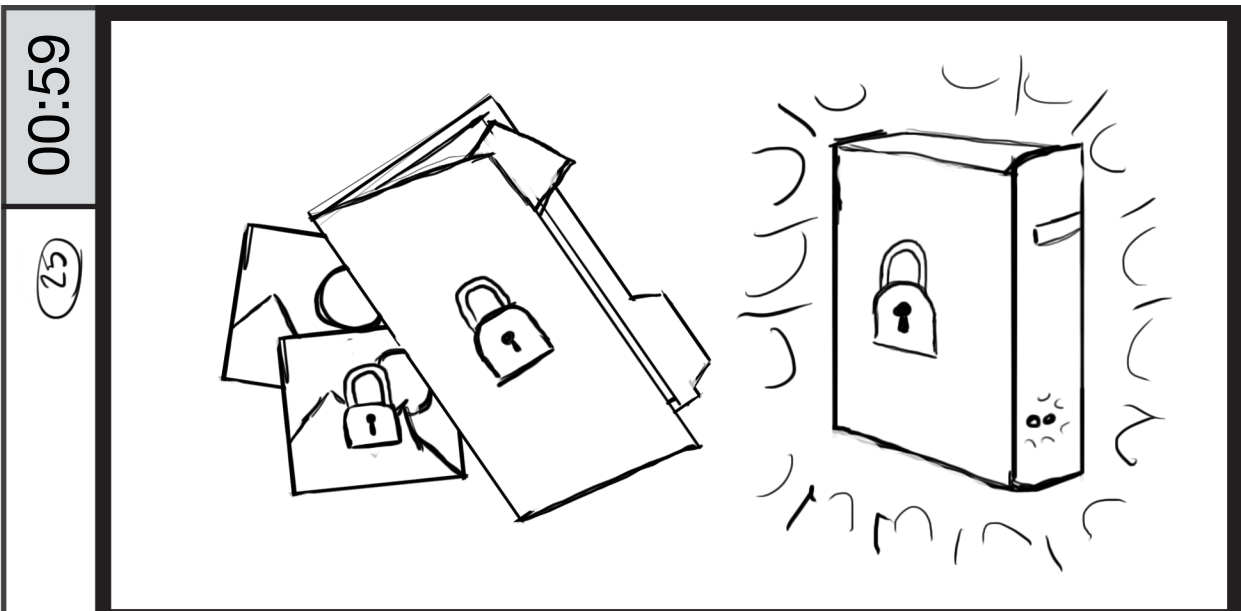


Ransom money falls into the net (animated in from the right) from the top of the shot.

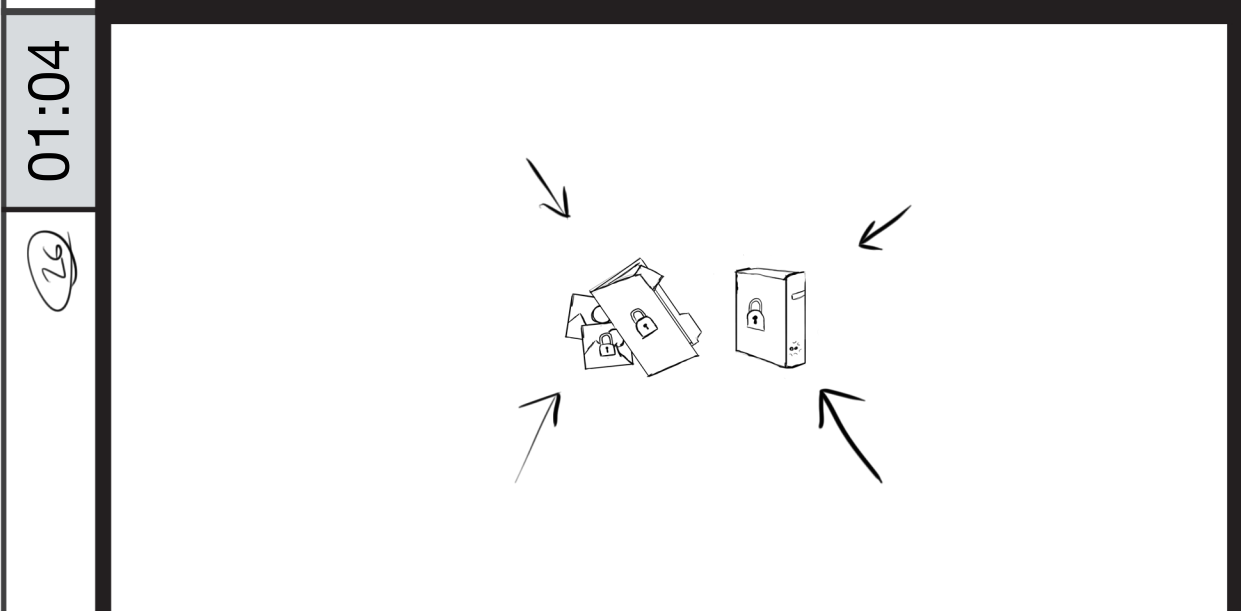


NARRATOR:

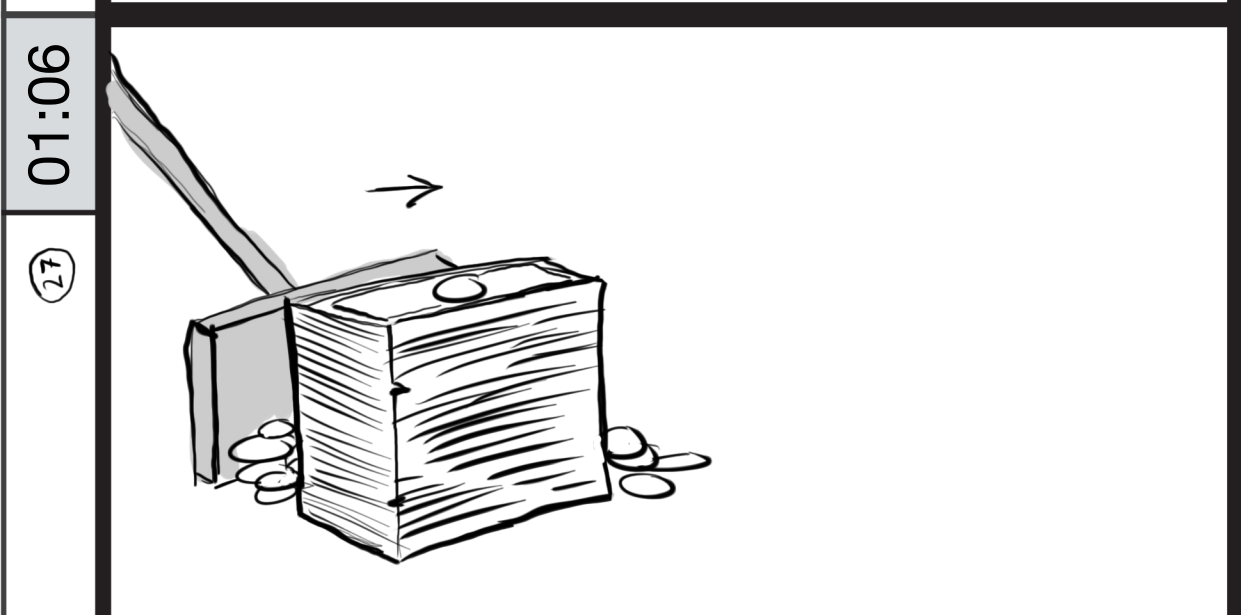
Any personal or company information is now compromised and files are inaccessible.



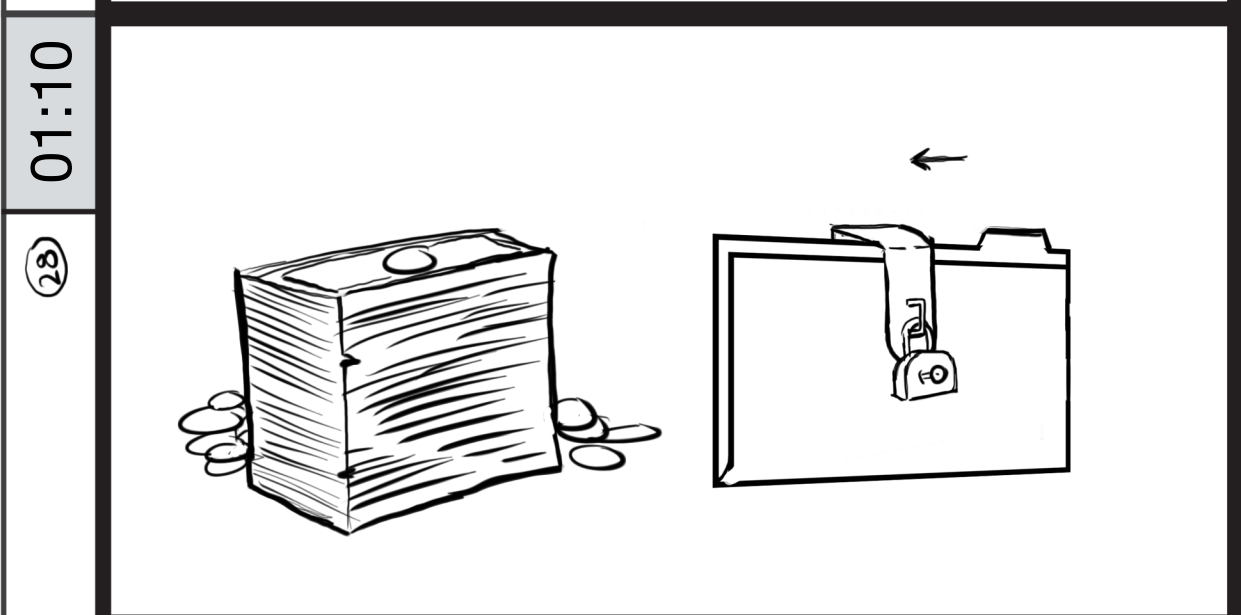
NARRATOR:
Ransomware can even affect backup drives or other computers in your network.



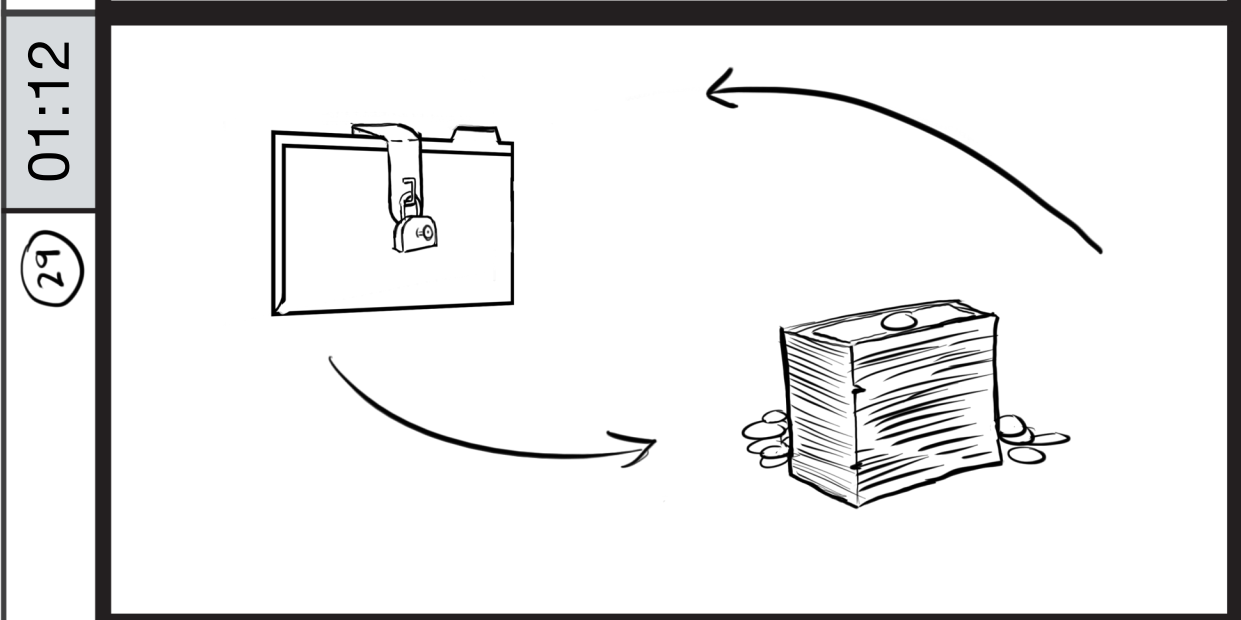
Both elements scale down and out in the middle of the shot.



NARRATOR:
If you pay the ransom, you assume attackers will stay true to their word.

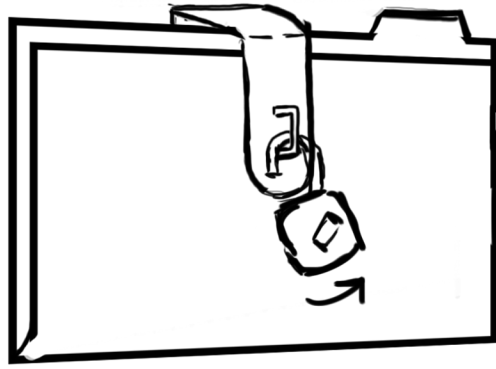


NARRATOR:
There is never a guarantee that you will get all of your files back after paying the ransom.



01:18

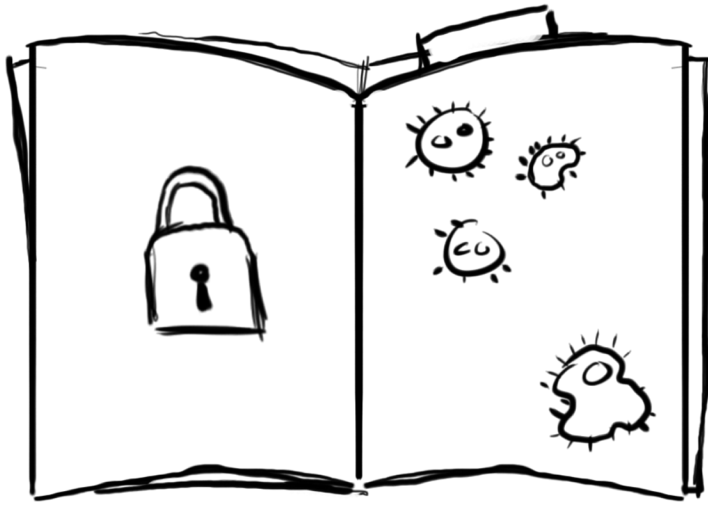
30



A key inserts itself into the padlock unlocking the files.

01:23

31

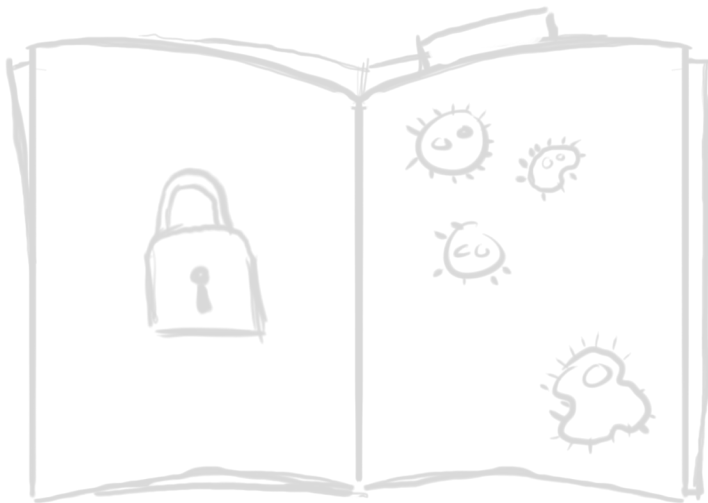


NARRATOR:

Also, attackers are likely to leave other malicious files behind.

01:28

32

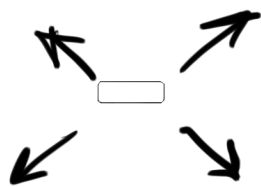


NARRATOR:

It's difficult to recover your files once they're encrypted, so the best time to stop a ransomware attack is before it happens.

01:30

33



A button begins to scale into the shot with a bounce ease-in animation.

01:32

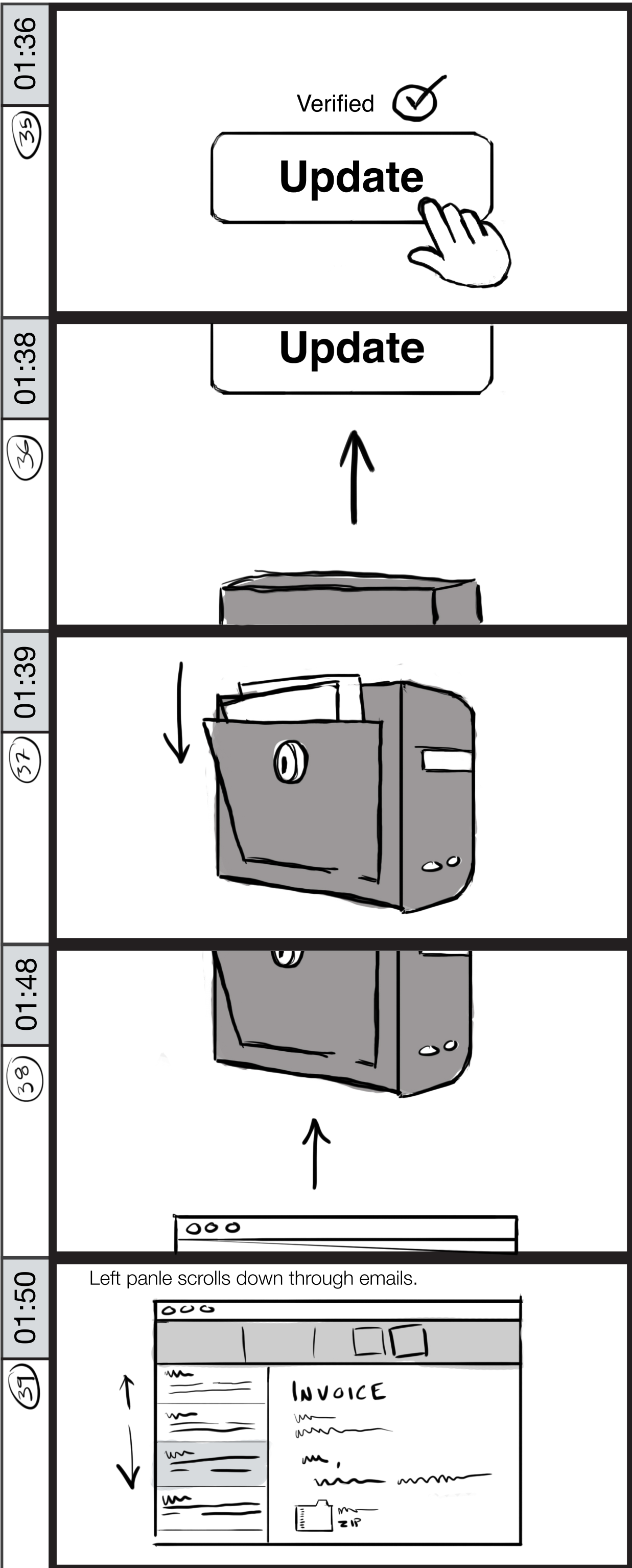
34



NARRATOR:

Update software frequently. Unpatched software can contain security holes, used to gain access into your system.

The verified identifier doesn't appear until the update button comes into focus.

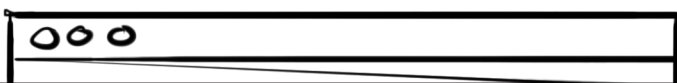
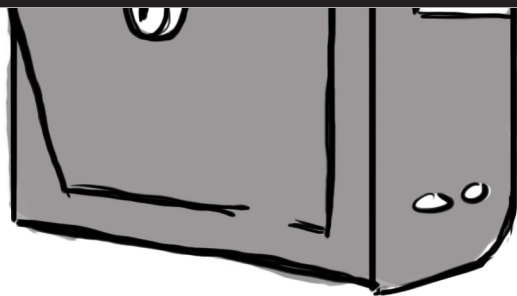
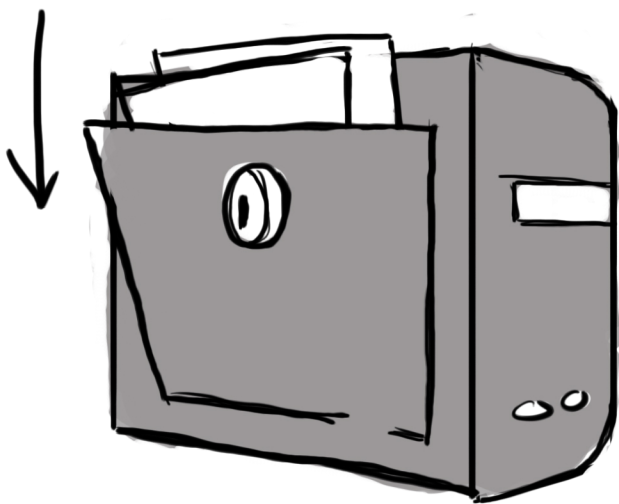


Verified ✓

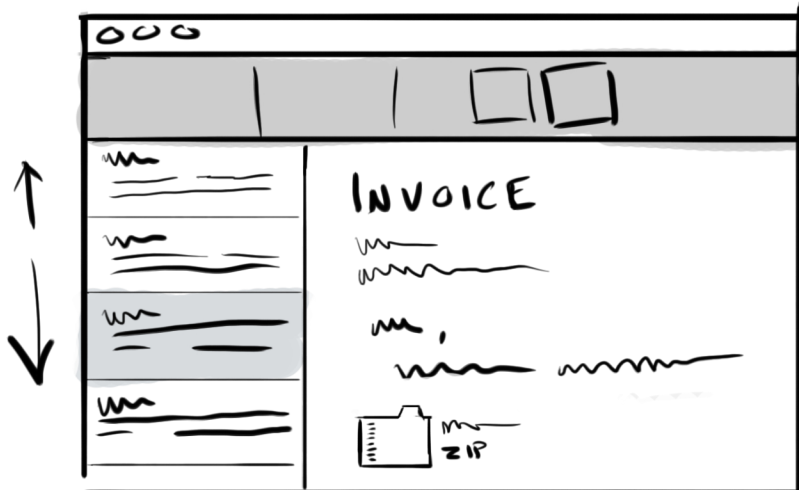
Update



Update



Left panle scrolls down through emails.



NARRATOR:

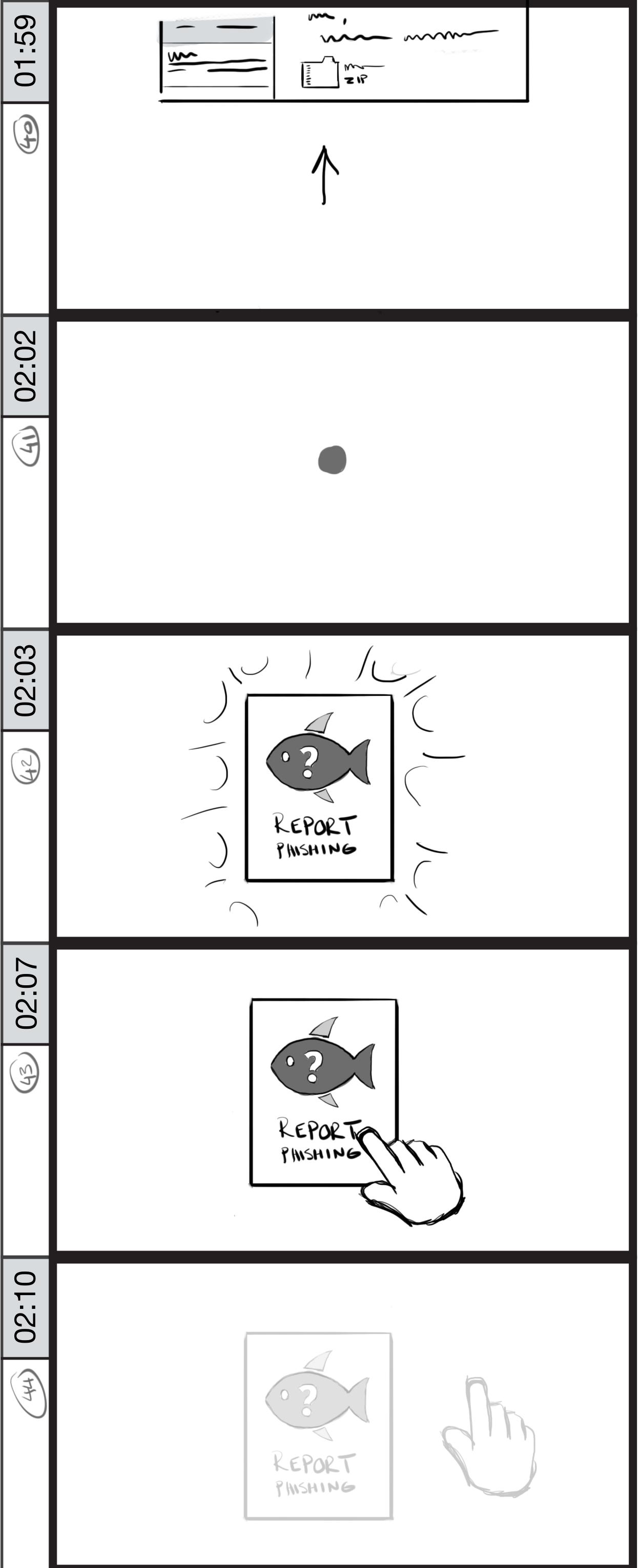
Back up your files regularly. Secure your backup in a safe place and disconnect it from your computer when you aren't using it.

The side container of the backup drive opens hinging from the bottom and a set of files drop down into the opening.

NARRATOR:

Use caution while surfing the web and checking your inbox. Never download attachments or click any links from unknown senders.

The information in the email client is block designed similar to previous videos.



NARRATOR:
And finally, report any suspicious email to keep our organization's information safe and secure.