GLOBAL THREATS TO LOCAL BUSINESS: **EMAIL COMPROMISE & RANSOMWARE**

What is the Threat?

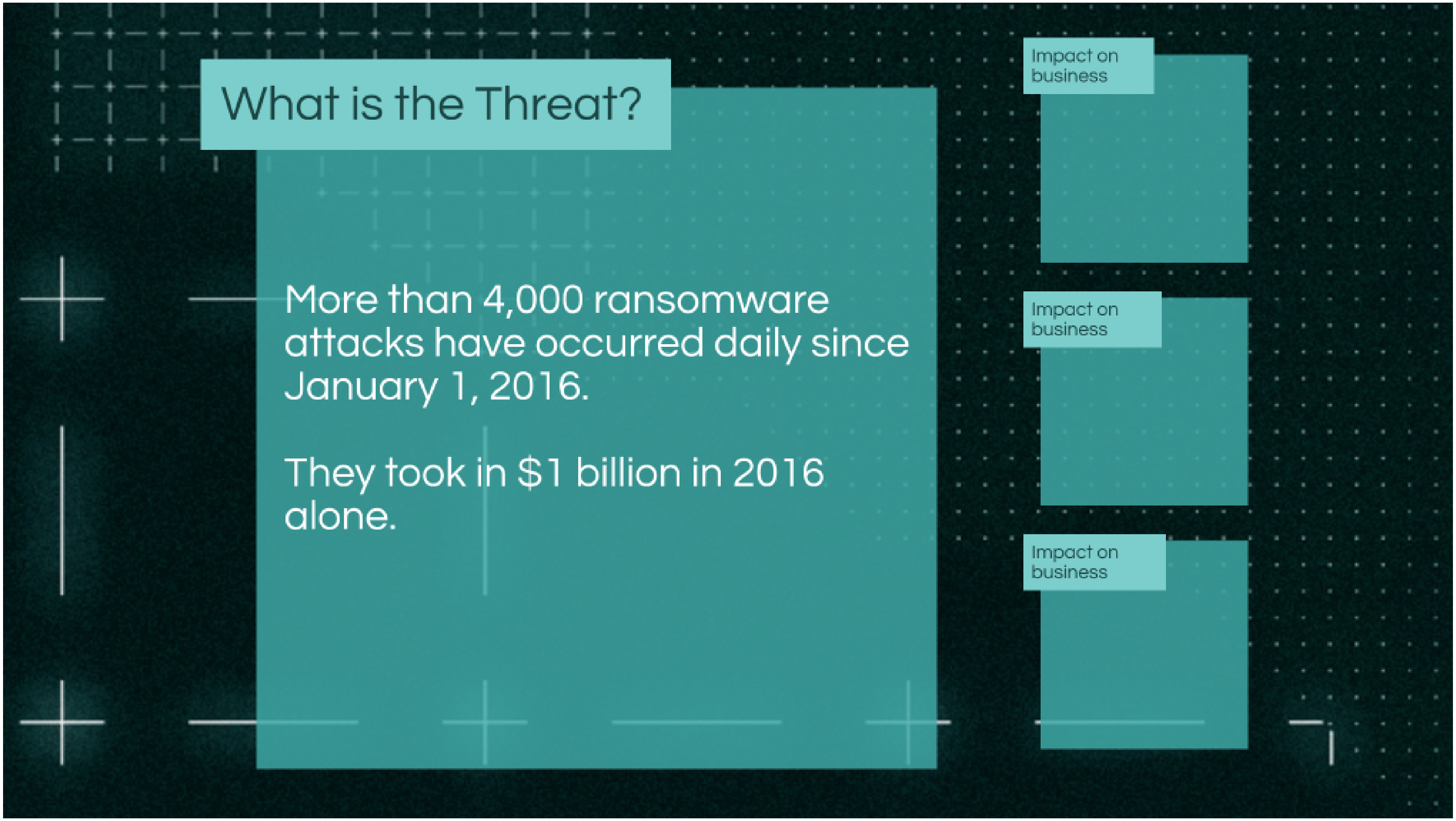
Overview

Business Email Compromise

Ransomware

Conclusion

A public service by
The San Mateo County
District Attorney's Office



What is the Threat?

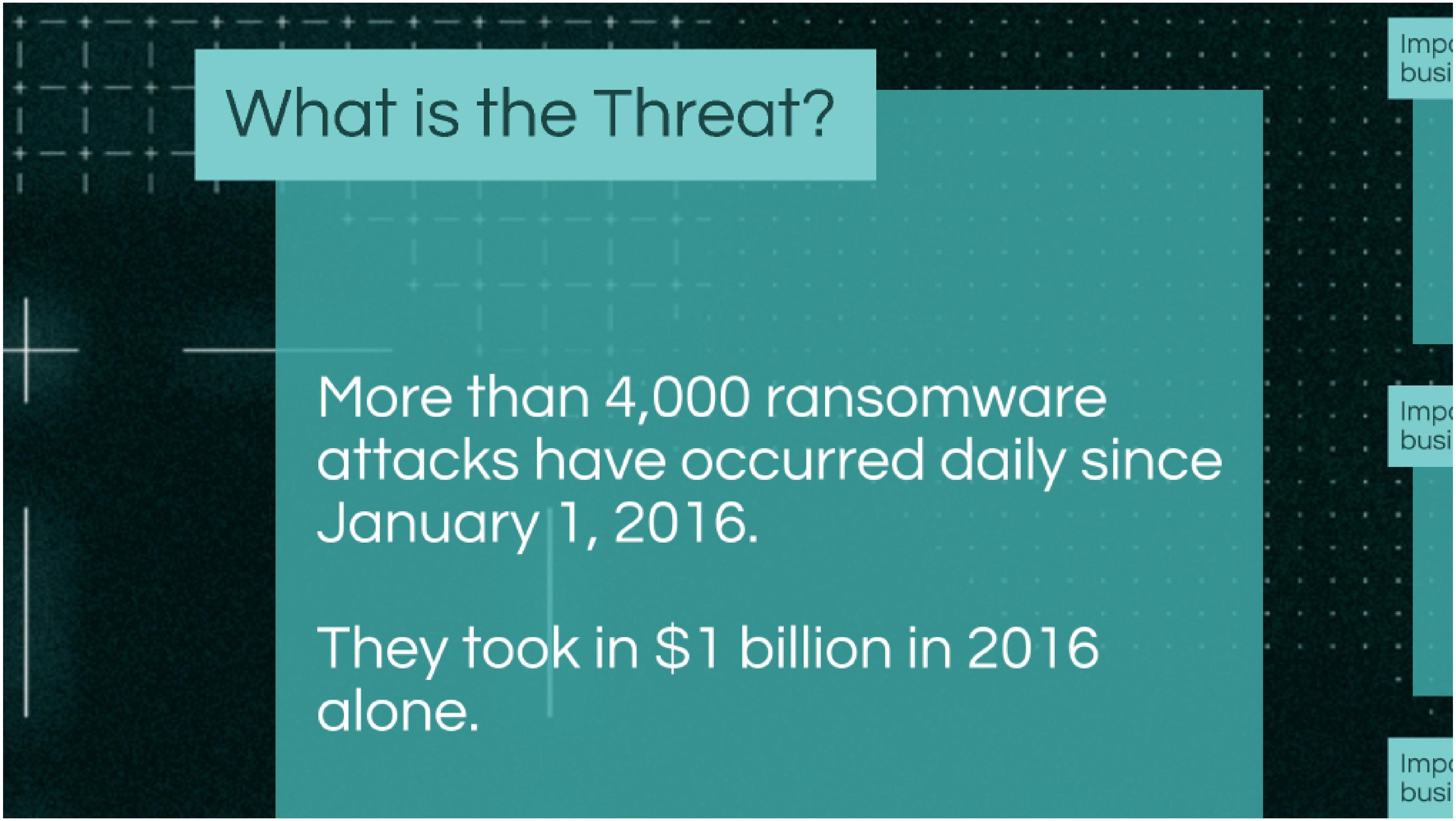
More than 4,000 ransomware attacks have occurred daily since January 1, 2016.

They took in $1 billion in 2016 alone.

Impact on business

Impact on business

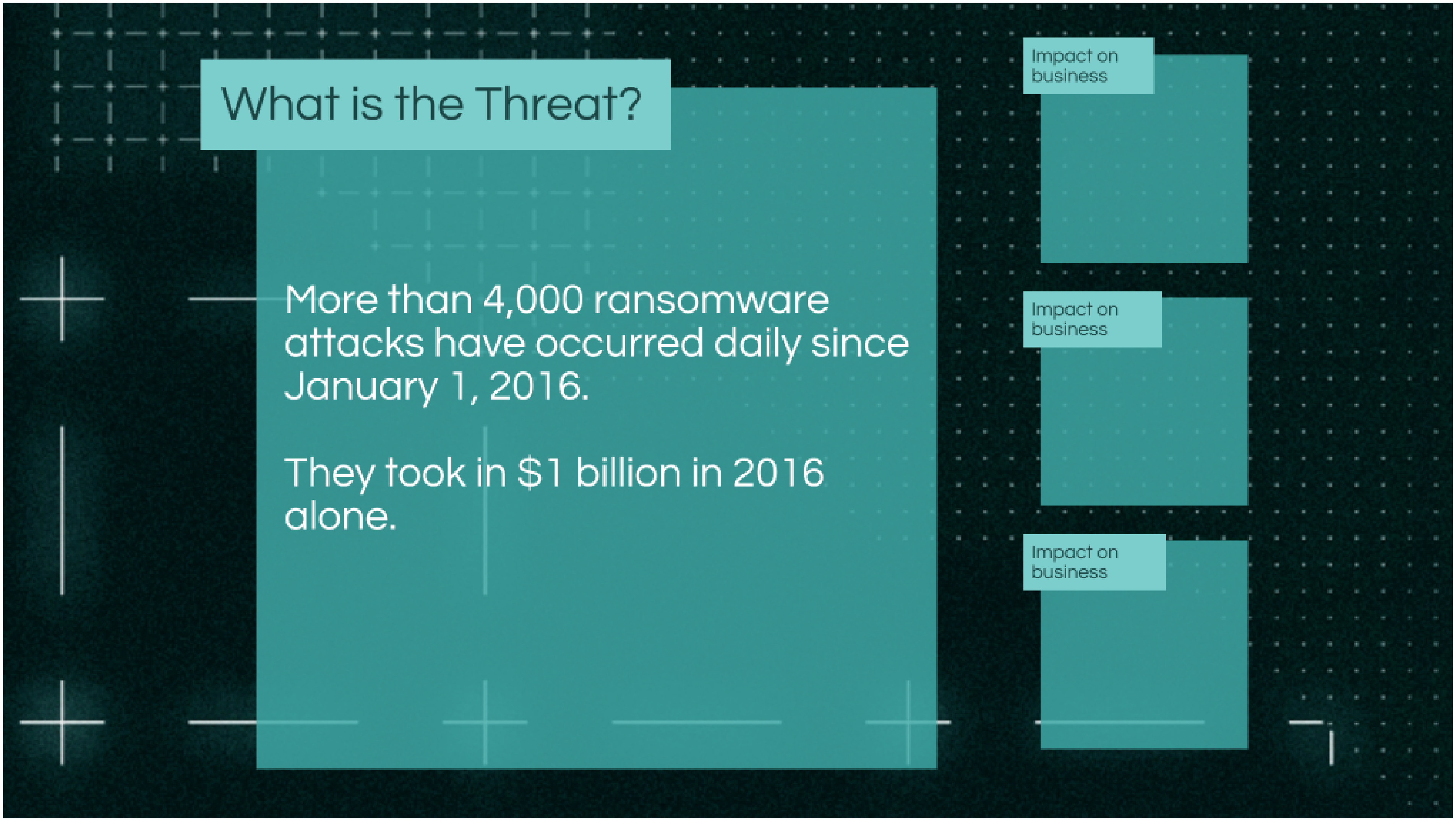
Impact on business



What is the Threat?

More than 4,000 ransomware attacks have occurred daily since January 1, 2016.

They took in $1 billion in 2016 alone.



What is the Threat?

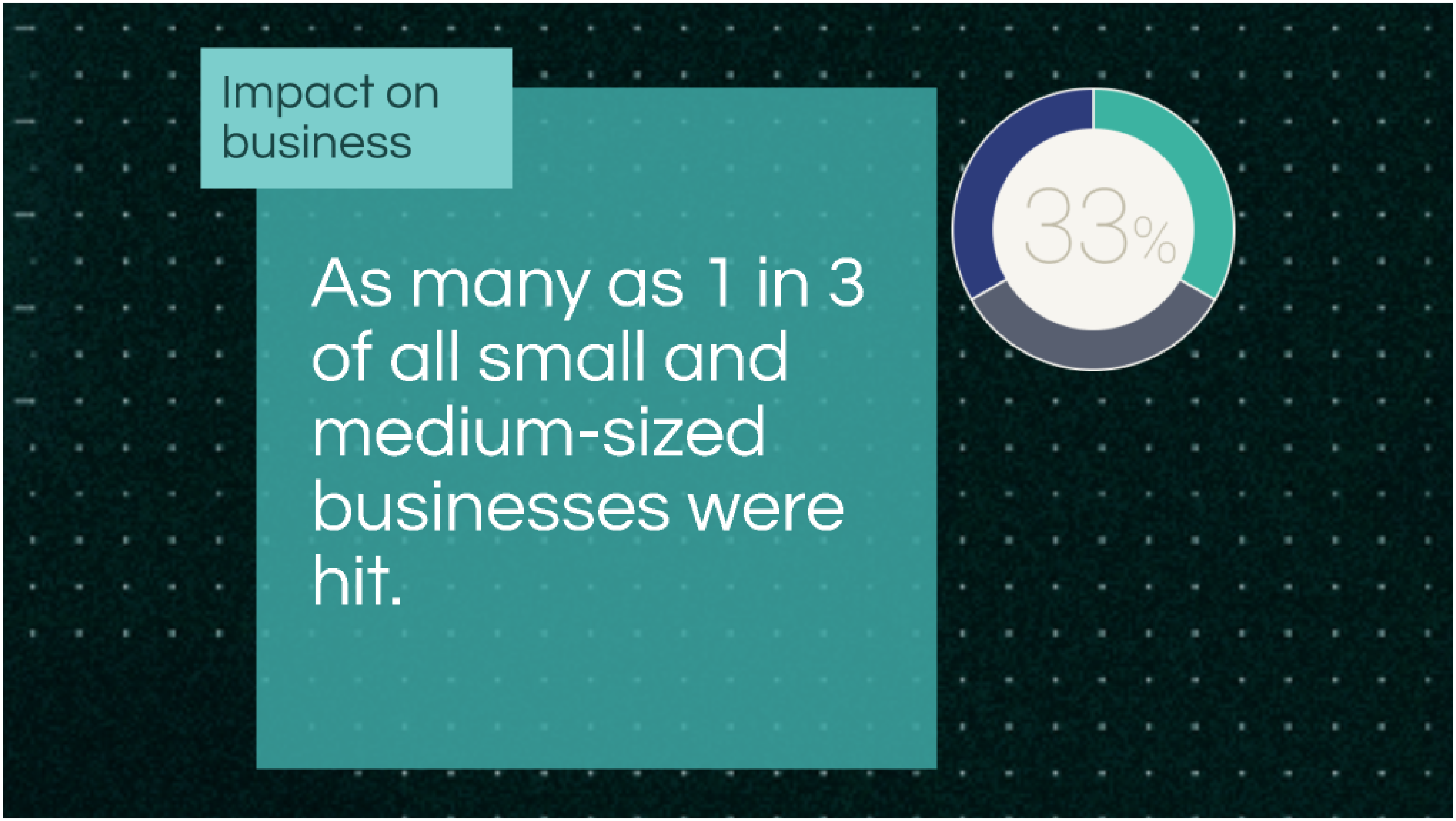
More than 4,000 ransomware attacks have occurred daily since January 1, 2016.

They took in $1 billion in 2016 alone.

Impact on business

Impact on business

Impact on business

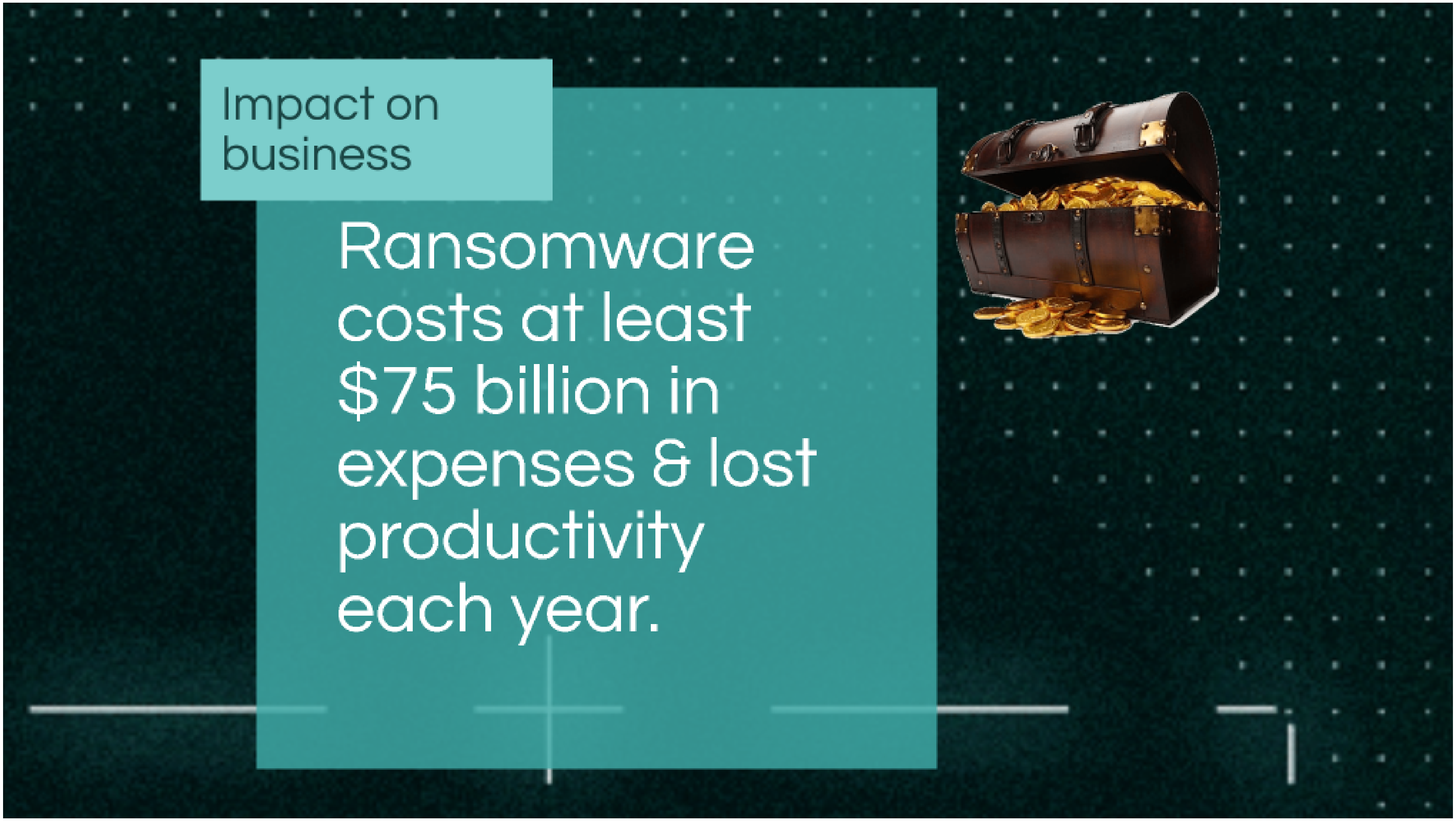


Impact on business

As many as 1 in 3 of all small and medium-sized businesses were hit.

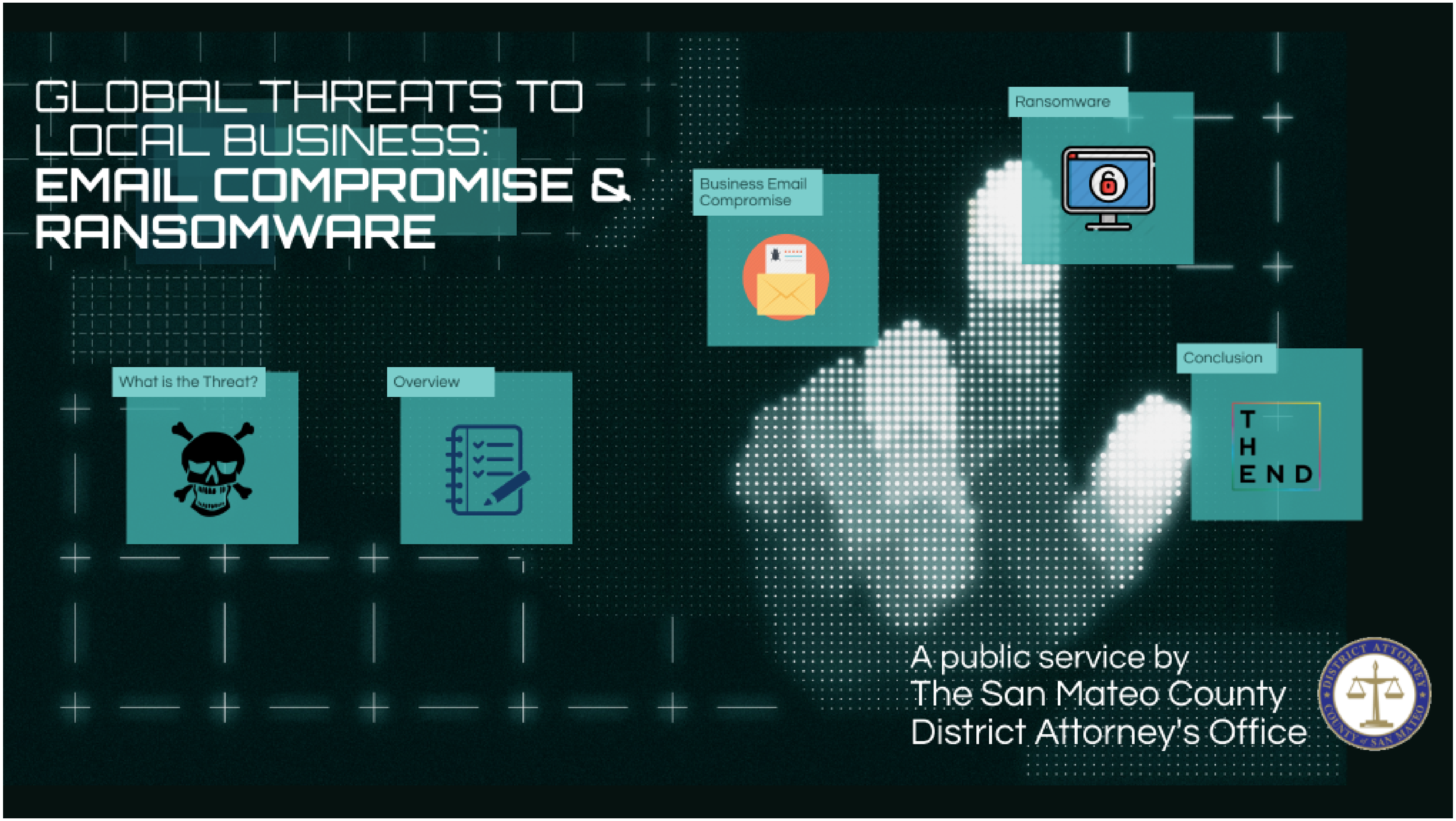
Impact on business

1 in 5 businesses that were hit had to completely shut down operations.



Impact on business

Ransomware costs at least $75 billion in expenses & lost productivity each year.



GLOBAL THREATS TO LOCAL BUSINESS: **EMAIL COMPROMISE & RANSOMWARE**

What is the Threat?

Overview

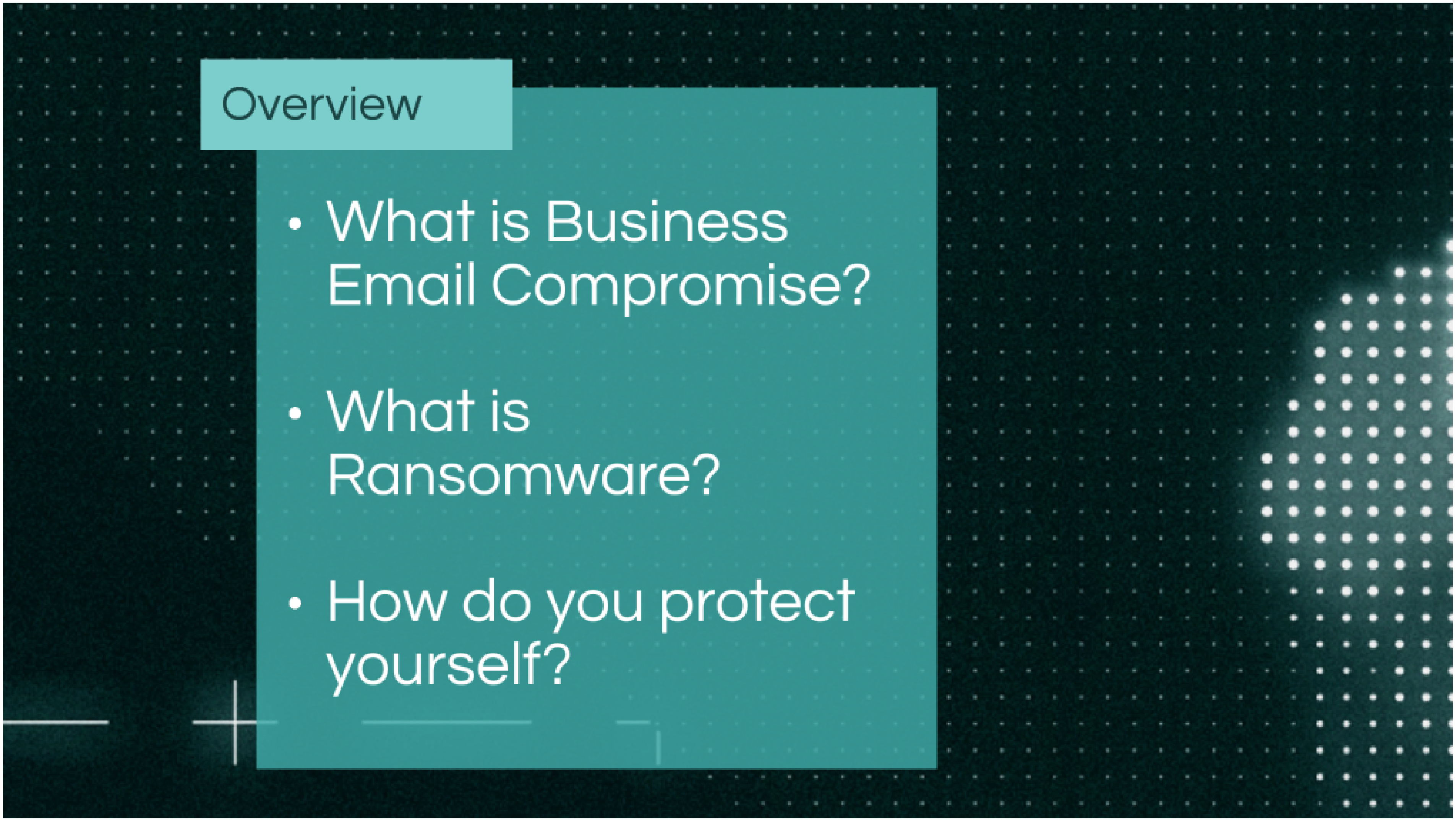
Business Email Compromise

Ransomware

Conclusion

T
H
END

A public service by
The San Mateo County
District Attorney's Office



Overview

- What is Business Email Compromise?
- What is Ransomware?
- How do you protect yourself?

GLOBAL THREATS TO LOCAL BUSINESS: **EMAIL COMPROMISE & RANSOMWARE**

What is the Threat?

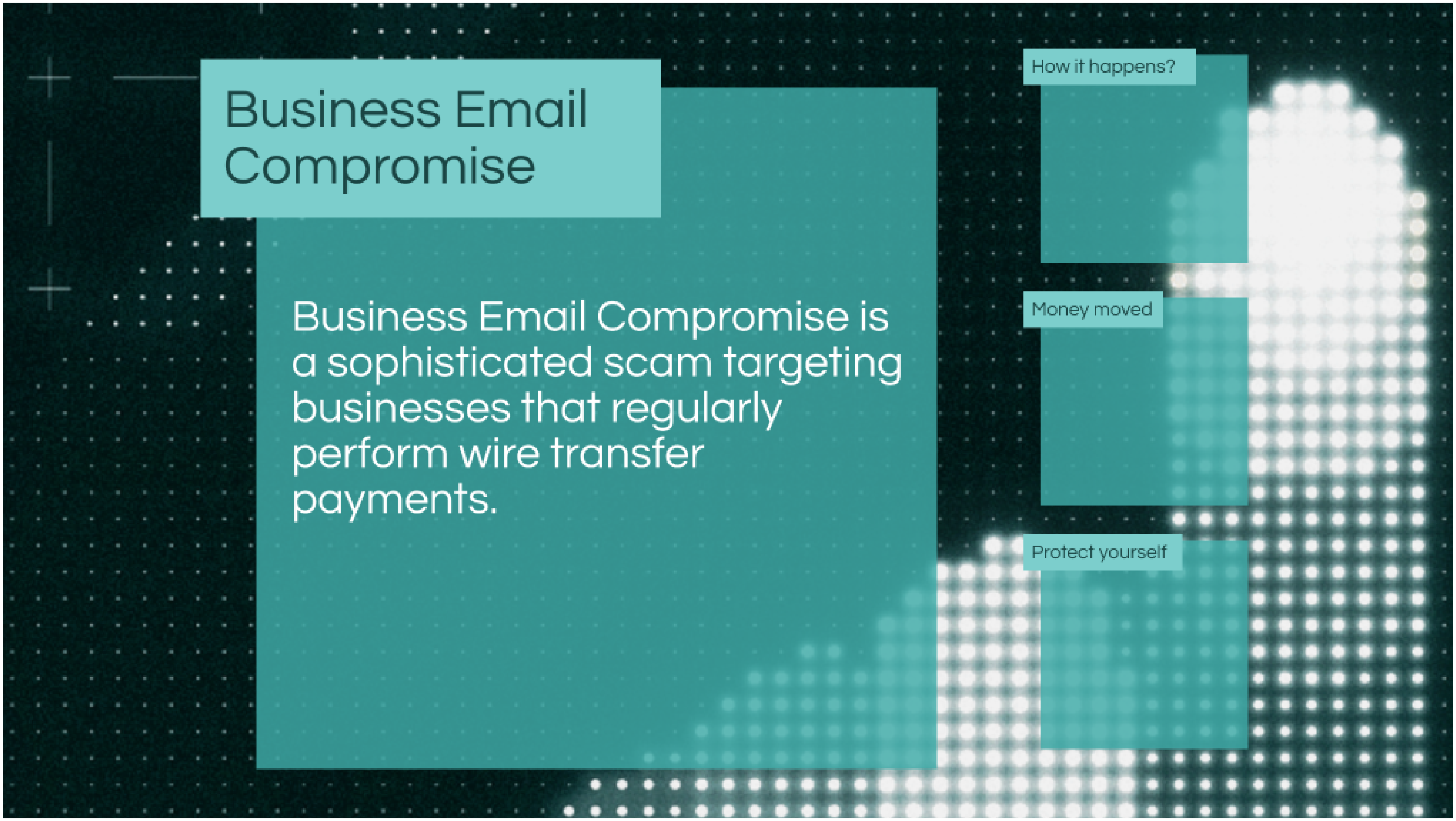
Overview

Business Email Compromise

Ransomware

Conclusion

A public service by
The San Mateo County
District Attorney's Office



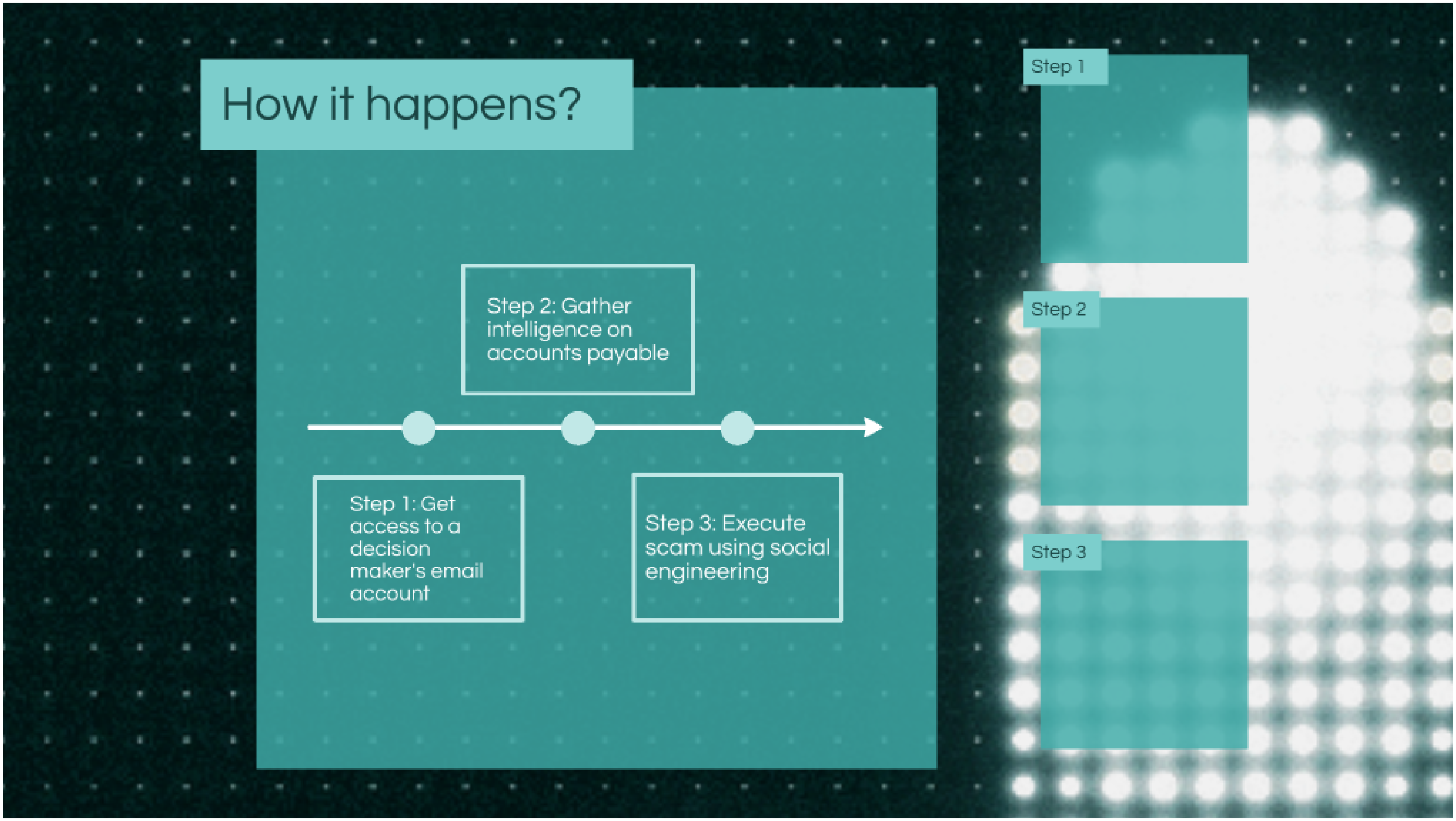
Business Email Compromise

Business Email Compromise is a sophisticated scam targeting businesses that regularly perform wire transfer payments.

How it happens?

Money moved

Protect yourself



How it happens?

Step 2: Gather intelligence on accounts payable

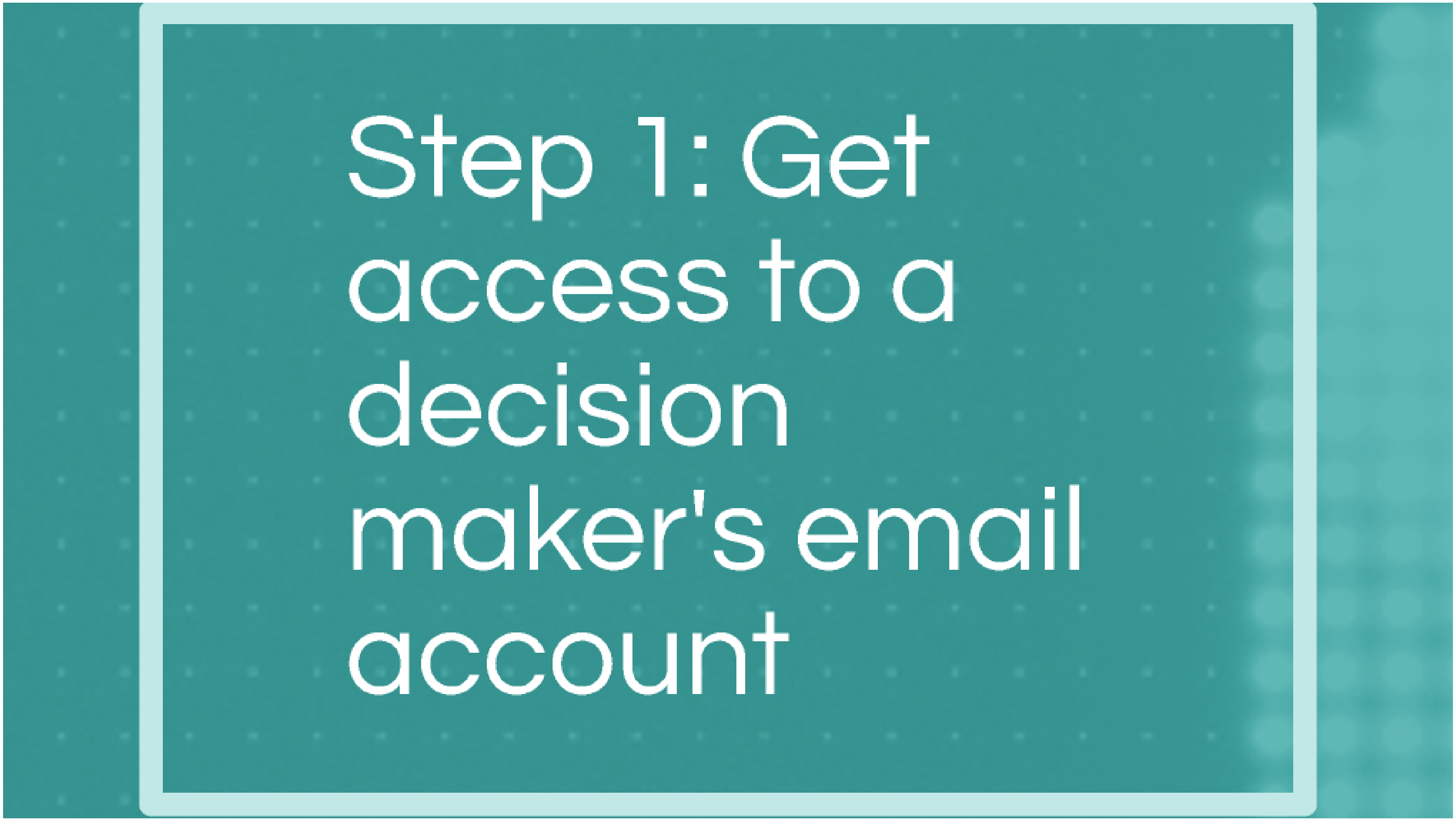
Step 1: Get access to a decision maker's email account

Step 3: Execute scam using social engineering

Step 1

Step 2

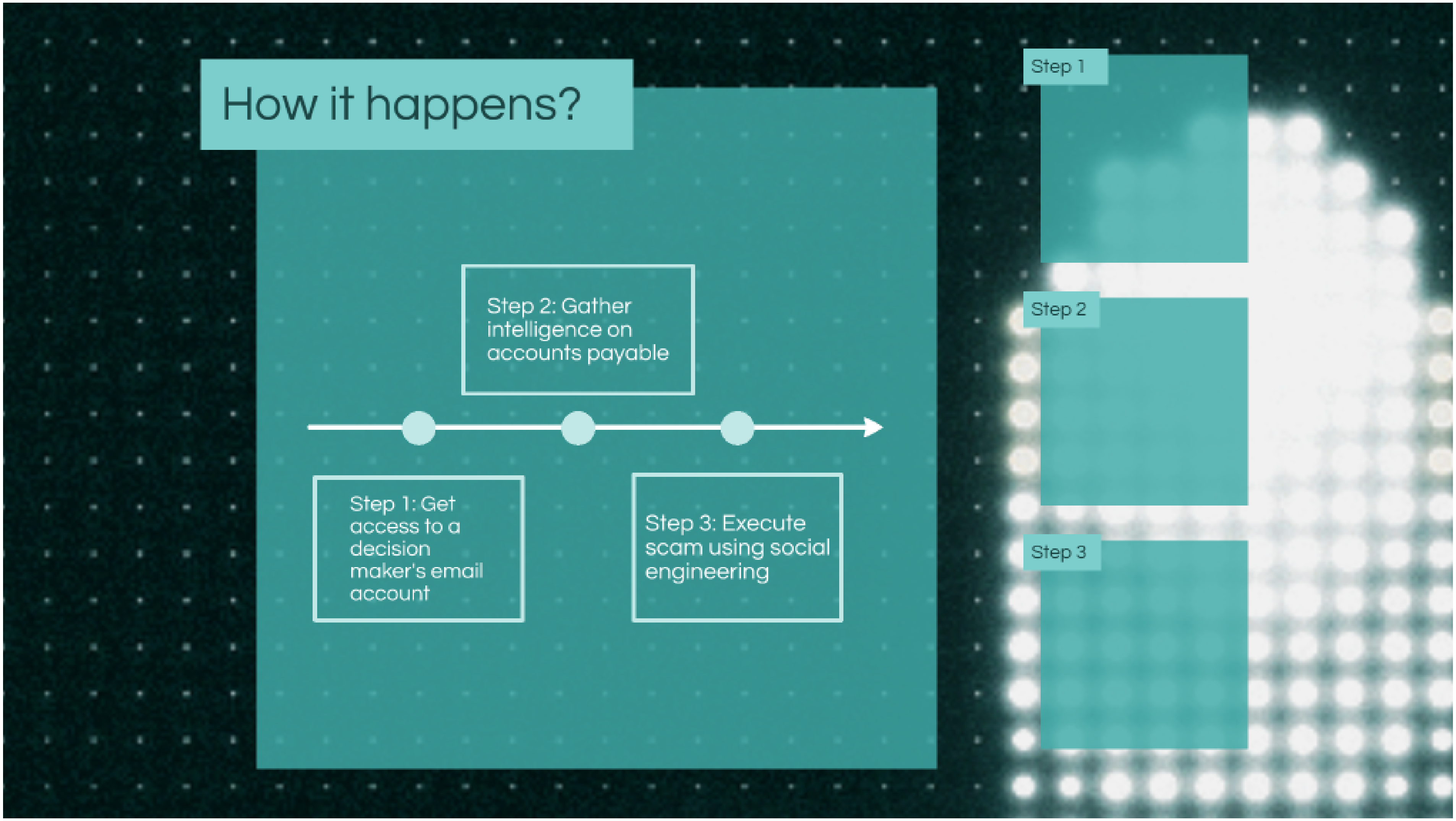
Step 3



Step 1: Get access to a decision maker's email account

Step 2: Gather intelligence on accounts payable

Step 3: Execute scam using social engineering



How it happens?

Step 1: Get access to a decision maker's email account

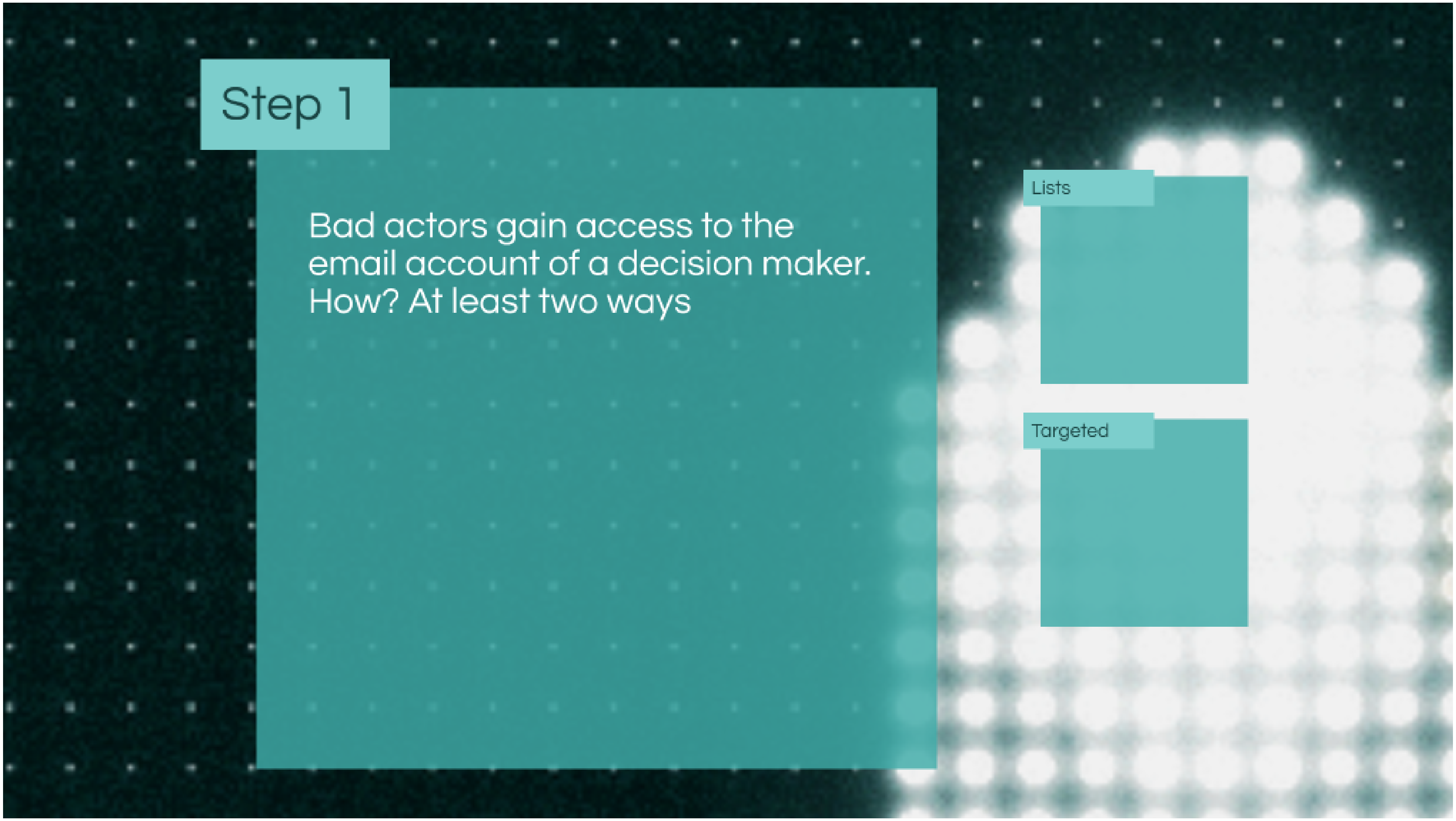
Step 2: Gather intelligence on accounts payable

Step 3: Execute scam using social engineering

Step 1

Step 2

Step 3

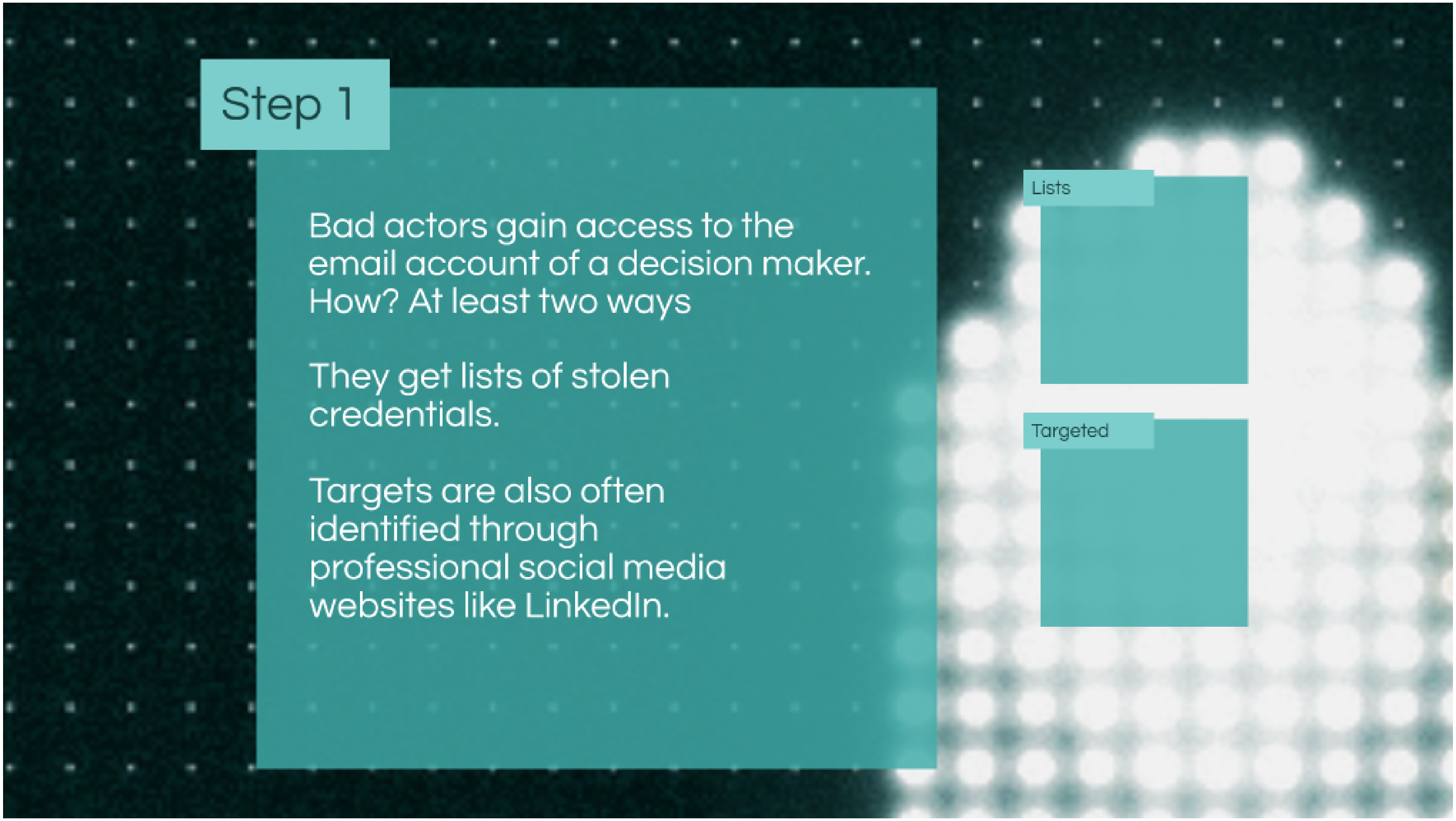


Step 1

Bad actors gain access to the email account of a decision maker. How? At least two ways

Lists

Targeted



Step 1

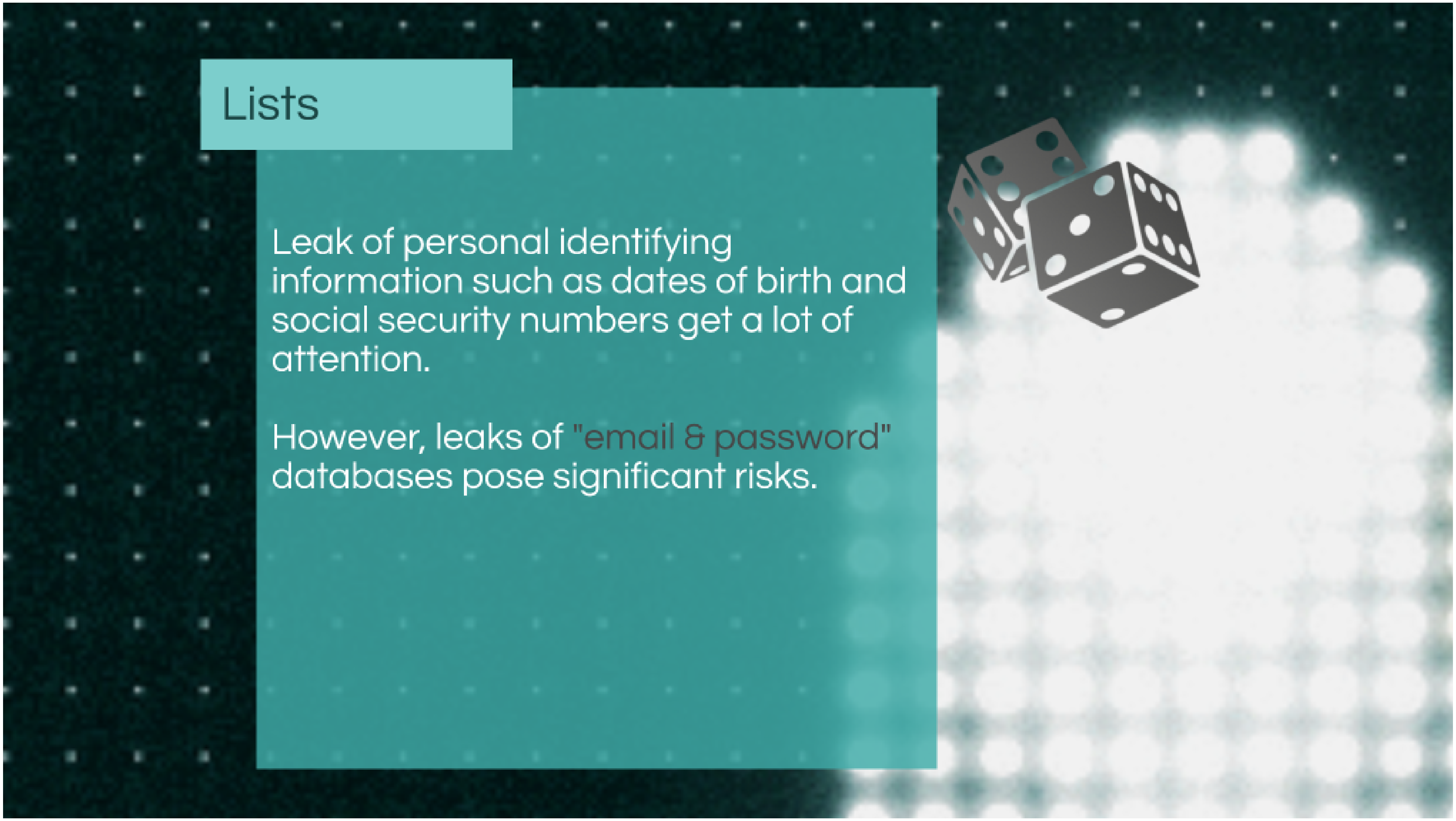
Bad actors gain access to the email account of a decision maker. How? At least two ways

They get lists of stolen credentials.

Targets are also often identified through professional social media websites like LinkedIn.

Lists

Targeted

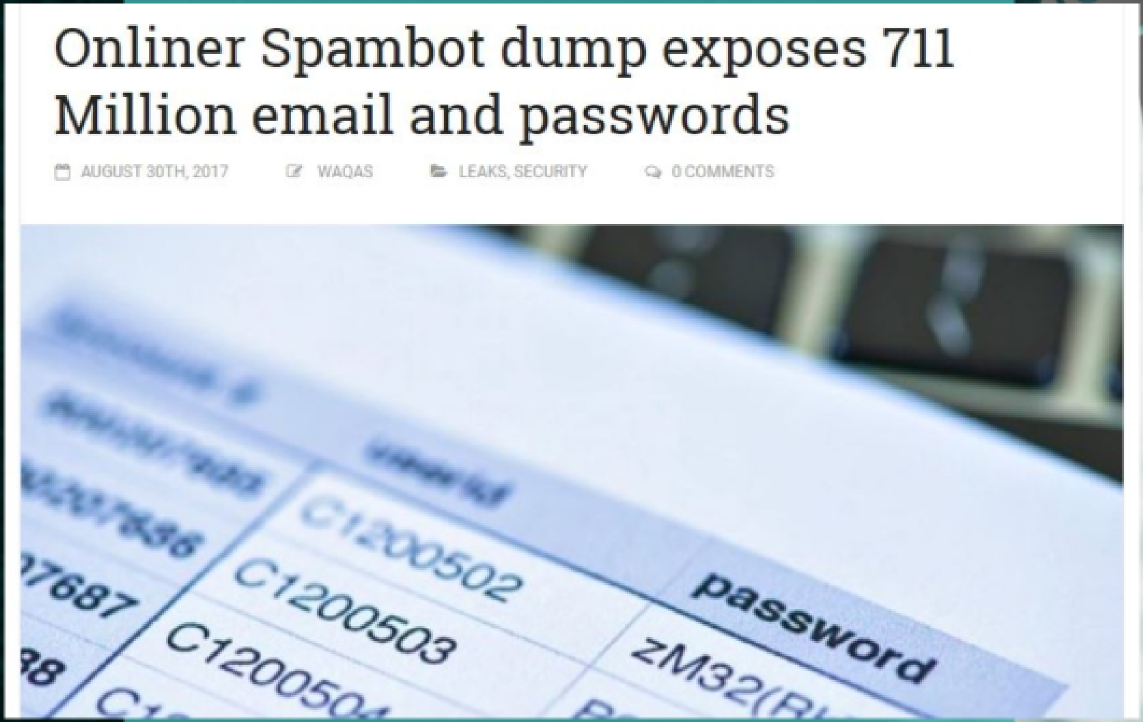


Lists

Leak of personal identifying information such as dates of birth and social security numbers get a lot of attention.

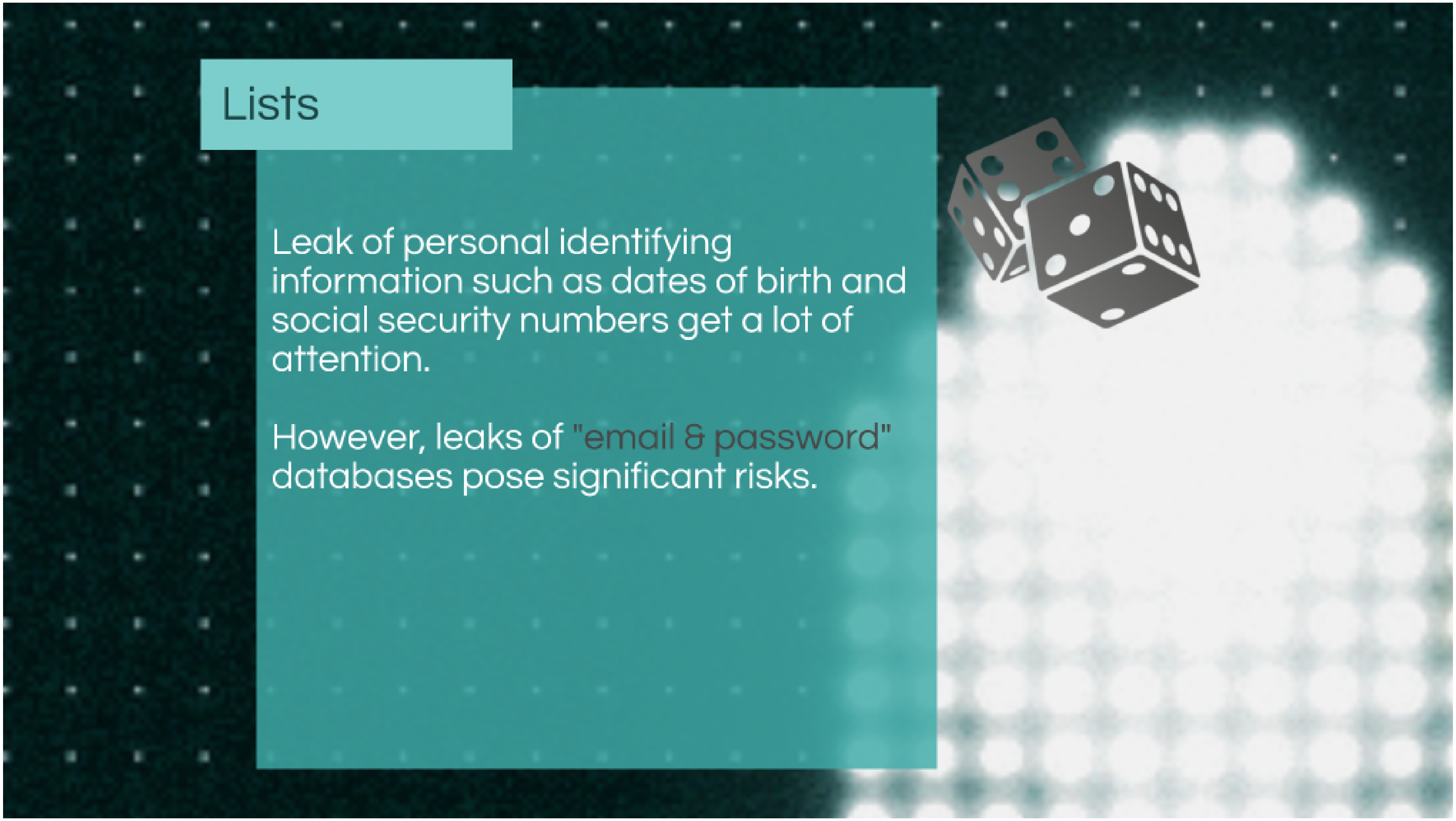
However, leaks of "email & password" databases pose significant risks.

Lists



Onliner Spambot dump exposes 711 Million email and passwords

AUGUST 30TH, 2017 WAQAS LEAKS, SECURITY 0 COMMENTS

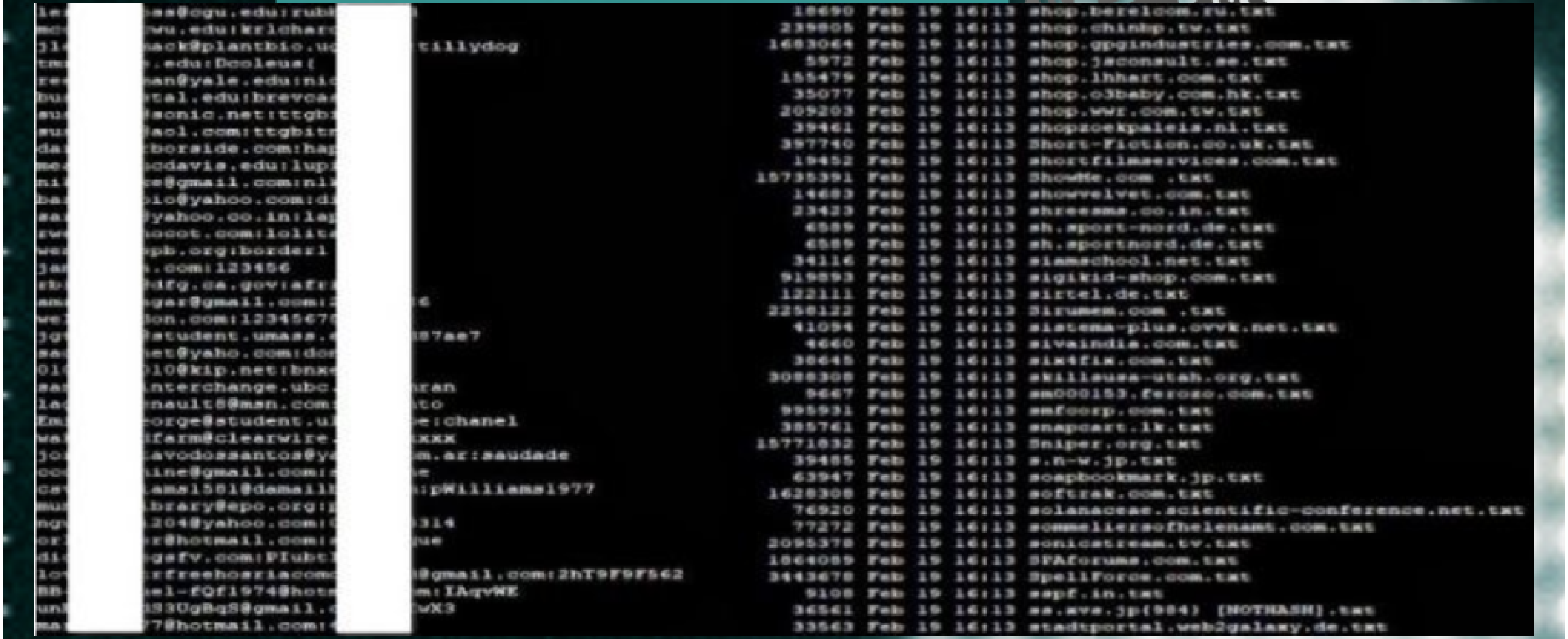


Lists

Leak of personal identifying information such as dates of birth and social security numbers get a lot of attention.

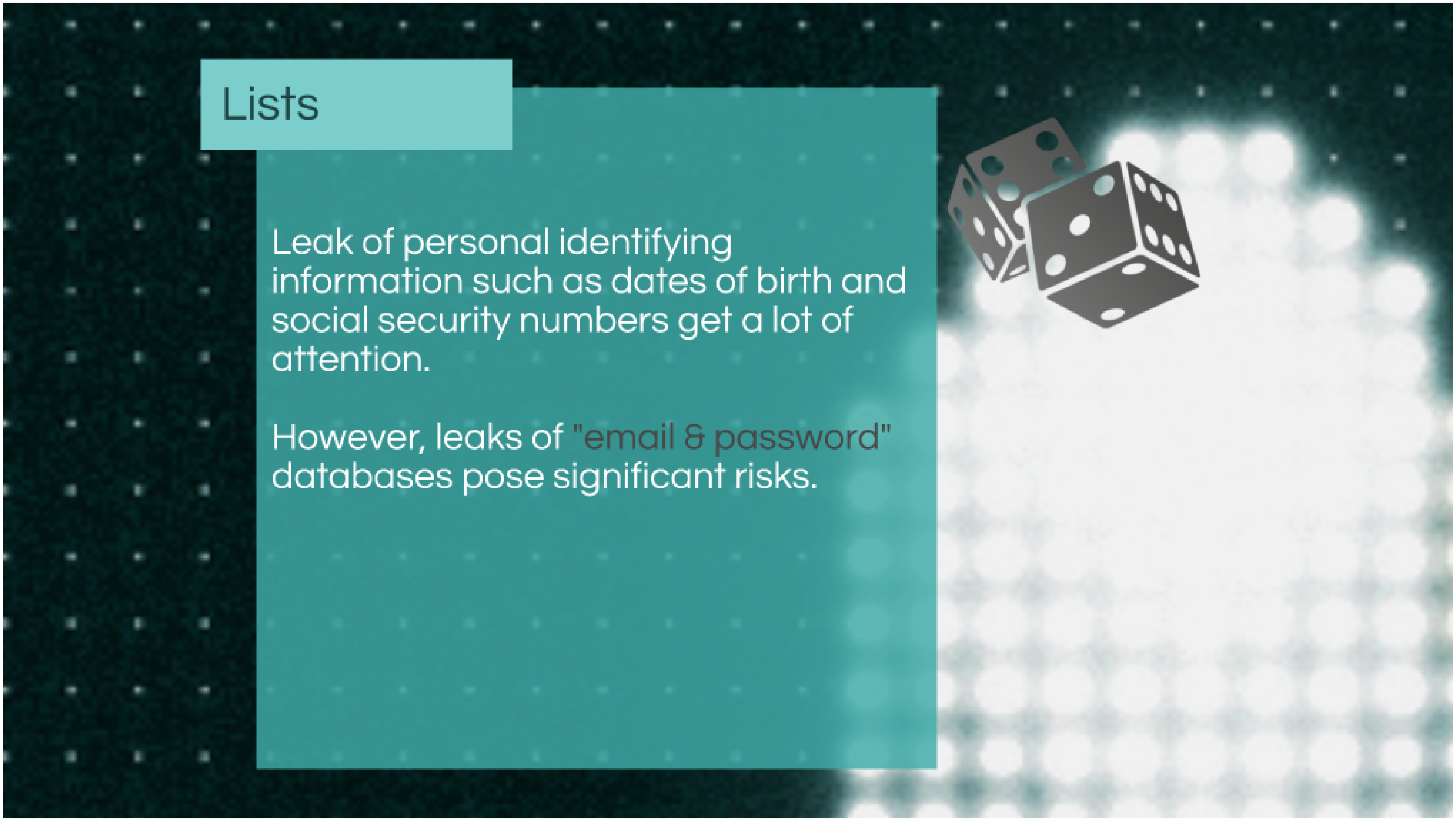
However, leaks of "email & password" databases pose significant risks.

Lists



```
le[redacted]as@cgu.edu:rubb[redacted]n
mc[redacted]wu.edu:krlchard[redacted]
j1[redacted]ack@plantbio.uc[redacted]tillydog
tm[redacted].edu:Dooleus(
re[redacted]an@yale.edu:nic
bu[redacted]tal.edu:brevca
su[redacted]@sonic.net:ttgb
su[redacted]@aol.com:ttgbit
da[redacted]borside.com:hap
me[redacted]cdavis.edu:lup
ni[redacted]e@gmail.com:ni
ba[redacted]io@yahoo.com:d
sa[redacted]yahoo.co.in:la
rw[redacted]ocot.com:lolit
we[redacted]pb.org:borderl
ja[redacted].com:123456
sb[redacted]dfg.ca.gov:afr
am[redacted]gar@gmail.com:[redacted]6
we[redacted]on.com:1234567[redacted]
jg[redacted]@student.umass.[redacted]87ae7
sa[redacted]et@yaho.com:do
01[redacted]10@kip.net:bnx
sa[redacted]nterchange.ubc.[redacted]ran
la[redacted]nault8@msn.com:[redacted]to
Em[redacted]orge@student.u[redacted]e:chanel
wa[redacted]farm@clearwire.[redacted]xxx
jo[redacted]avodossantos@y[redacted]m.ar:saudade
co[redacted]ine@gmail.com:[redacted]e
ca[redacted]ams1581@damaill[redacted]:pWilliams1977
mu[redacted]brary@epo.org:[redacted]
ng[redacted]204@yahoo.com:[redacted]314
or[redacted]r@hotmail.com:[redacted]ue
di[redacted]gsfv.com:PIubt[redacted]
lo[redacted]rfreehosrlacom[redacted]@gmail.com:2hT9F9F562
RB[redacted]el-fQf1974@hot[redacted]m:IAqvWE
un[redacted]S3UgBqS@gmail.[redacted]vX3
ma[redacted]7@hotmail.com:[redacted]
```

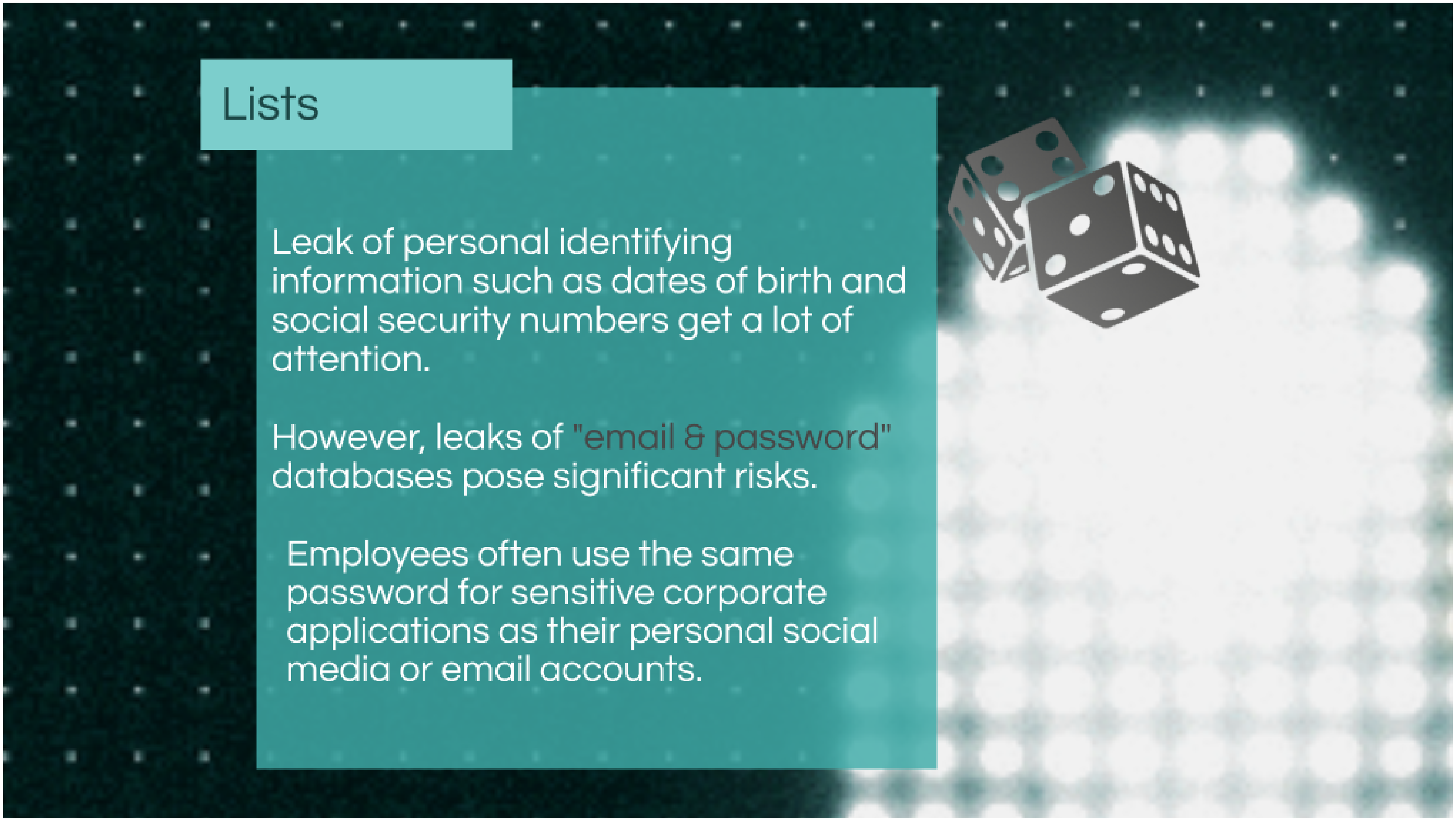
```
   18690 Feb 19 16:13 shop.berelcom.ru.txt
  239805 Feb 19 16:13 shop.chinbp.tw.txt
 1683064 Feb 19 16:13 shop.gpgindustries.com.txt
    5972 Feb 19 16:13 shop.jaconsult.se.txt
  155479 Feb 19 16:13 shop.lhhart.com.txt
   35077 Feb 19 16:13 shop.o3baby.com.hk.txt
  209203 Feb 19 16:13 shop.wwr.com.tw.txt
   39461 Feb 19 16:13 shopzoekpaleis.nl.txt
  397740 Feb 19 16:13 Short-Fiction.co.uk.txt
   19452 Feb 19 16:13 shortfilmservices.com.txt
15735391 Feb 19 16:13 ShowMe.com .txt
   14683 Feb 19 16:13 showvelvet.com.txt
   23423 Feb 19 16:13 shreesms.co.in.txt
    6589 Feb 19 16:13 sh.sport-nord.de.txt
    6589 Feb 19 16:13 sh.sportnord.de.txt
   34116 Feb 19 16:13 siamschool.net.txt
  919893 Feb 19 16:13 sigikid-shop.com.txt
  122111 Feb 19 16:13 sirtel.de.txt
 2256122 Feb 19 16:13 Sirumem.com .txt
   41094 Feb 19 16:13 sistema-plus.ovvk.net.txt
    4660 Feb 19 16:13 sivaindia.com.txt
   38645 Feb 19 16:13 sixtfix.com.txt
 3088308 Feb 19 16:13 skillsusa-utah.org.txt
    9667 Feb 19 16:13 sm000153.ferozo.com.txt
  995931 Feb 19 16:13 smfcorp.com.txt
  385761 Feb 19 16:13 snapcart.lk.txt
15771832 Feb 19 16:13 Sniper.org.txt
   39485 Feb 19 16:13 s.n-w.jp.txt
   63947 Feb 19 16:13 soapbookmark.jp.txt
 1628308 Feb 19 16:13 softrak.com.txt
   76920 Feb 19 16:13 solanaceae.scientific-conference.net.txt
   77272 Feb 19 16:13 sommeliersofhelenams.com.txt
 2095378 Feb 19 16:13 sonicstream.tv.txt
 1864089 Feb 19 16:13 SPAforums.com.txt
 3443678 Feb 19 16:13 SpellForce.com.txt
    9108 Feb 19 16:13 sspf.in.txt
   36561 Feb 19 16:13 ss.svs.jp(984) [NOTHASH].txt
   33563 Feb 19 16:13 stadtportal.web2galaxy.de.txt
```



Lists

Leak of personal identifying information such as dates of birth and social security numbers get a lot of attention.

However, leaks of "email & password" databases pose significant risks.

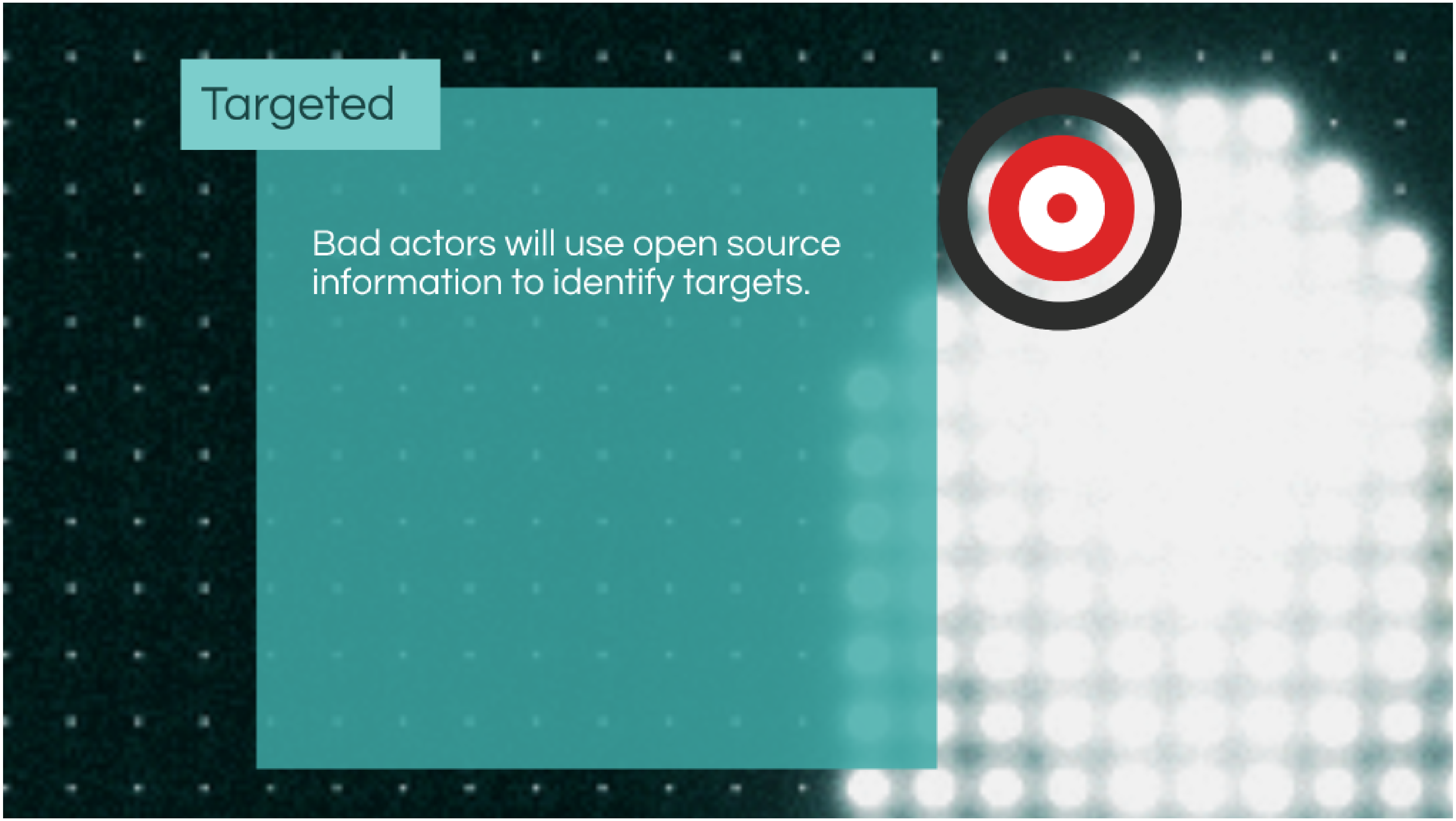


Lists

Leak of personal identifying information such as dates of birth and social security numbers get a lot of attention.

However, leaks of "email & password" databases pose significant risks.

Employees often use the same password for sensitive corporate applications as their personal social media or email accounts.

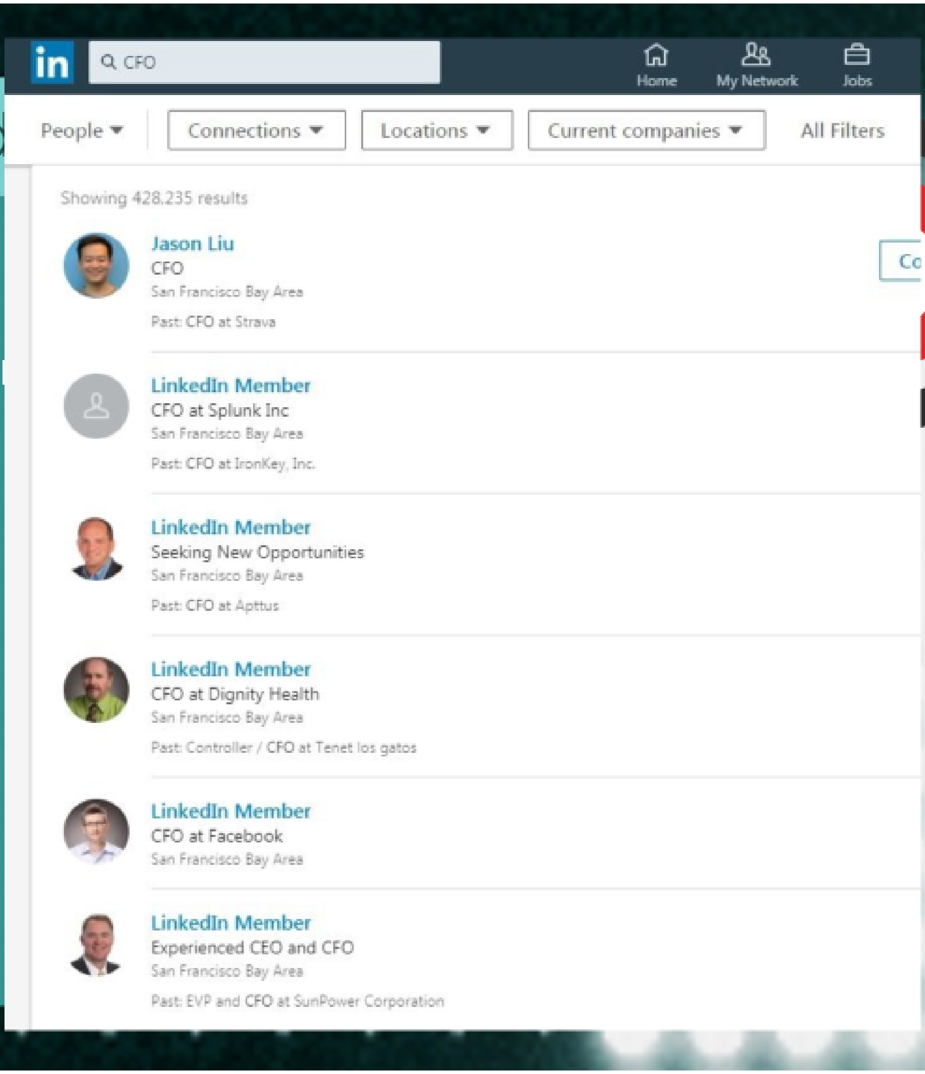


Targeted

Bad actors will use open source information to identify targets.

Targeted

Bad
infor



Showing 428,235 results

Jason Liu
CFO
San Francisco Bay Area
Past: CFO at Strava

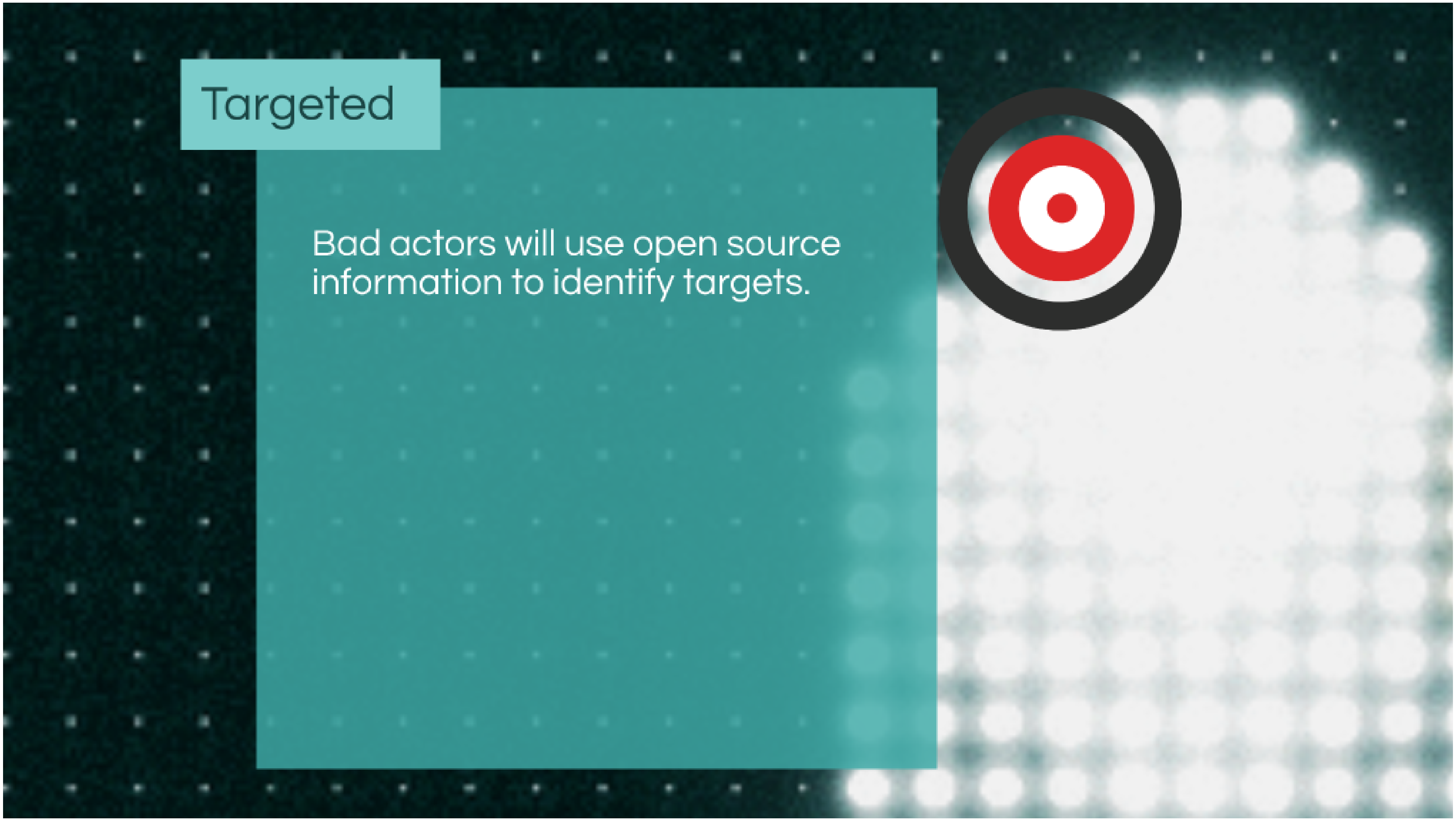
LinkedIn Member
CFO at Splunk Inc
San Francisco Bay Area
Past: CFO at IronKey, Inc.

LinkedIn Member
Seeking New Opportunities
San Francisco Bay Area
Past: CFO at Apttus

LinkedIn Member
CFO at Dignity Health
San Francisco Bay Area
Past: Controller / CFO at Tenet los gatos

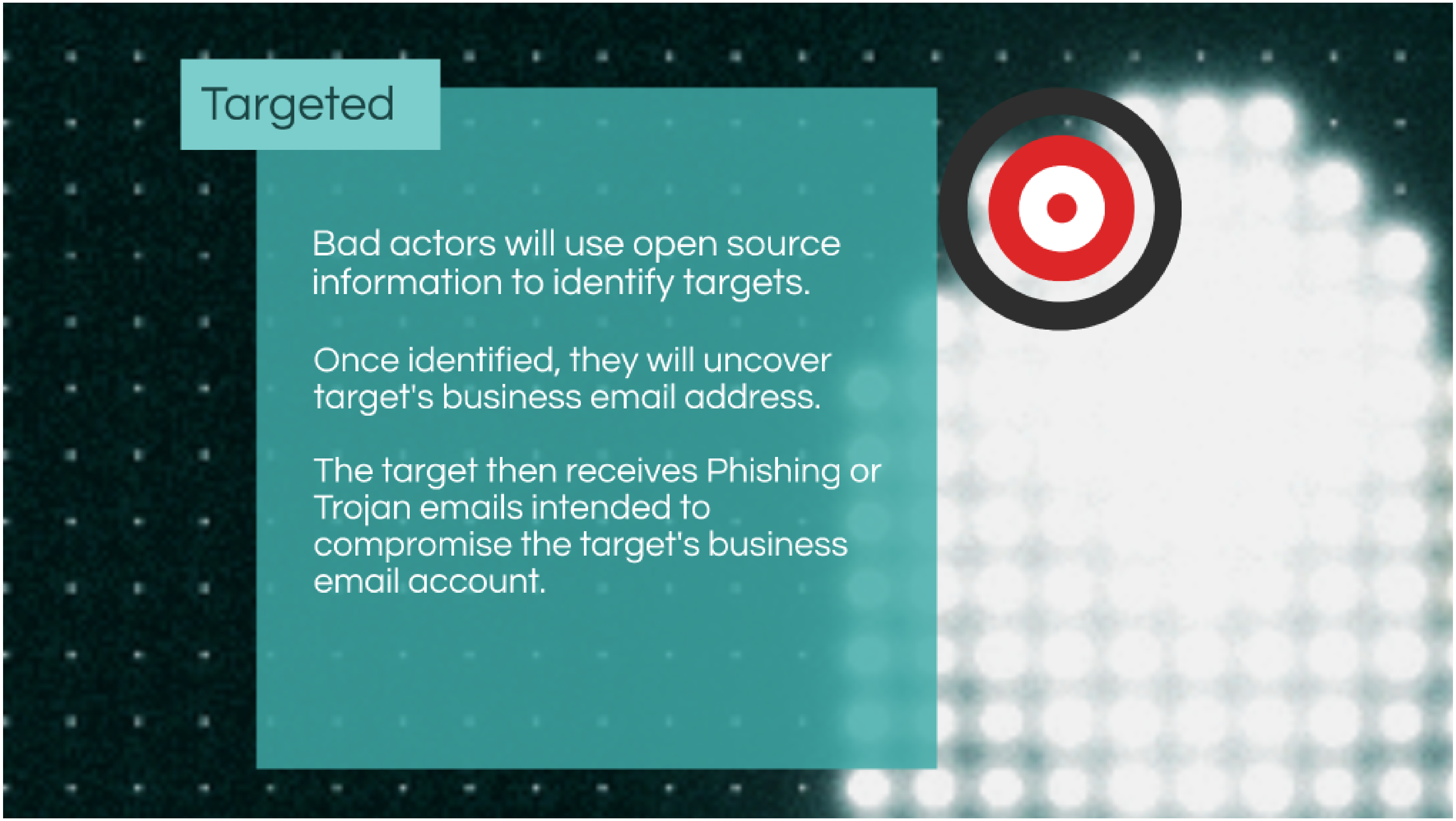
LinkedIn Member
CFO at Facebook
San Francisco Bay Area

LinkedIn Member
Experienced CEO and CFO
San Francisco Bay Area
Past: EVP and CFO at SunPower Corporation



Targeted

Bad actors will use open source information to identify targets.

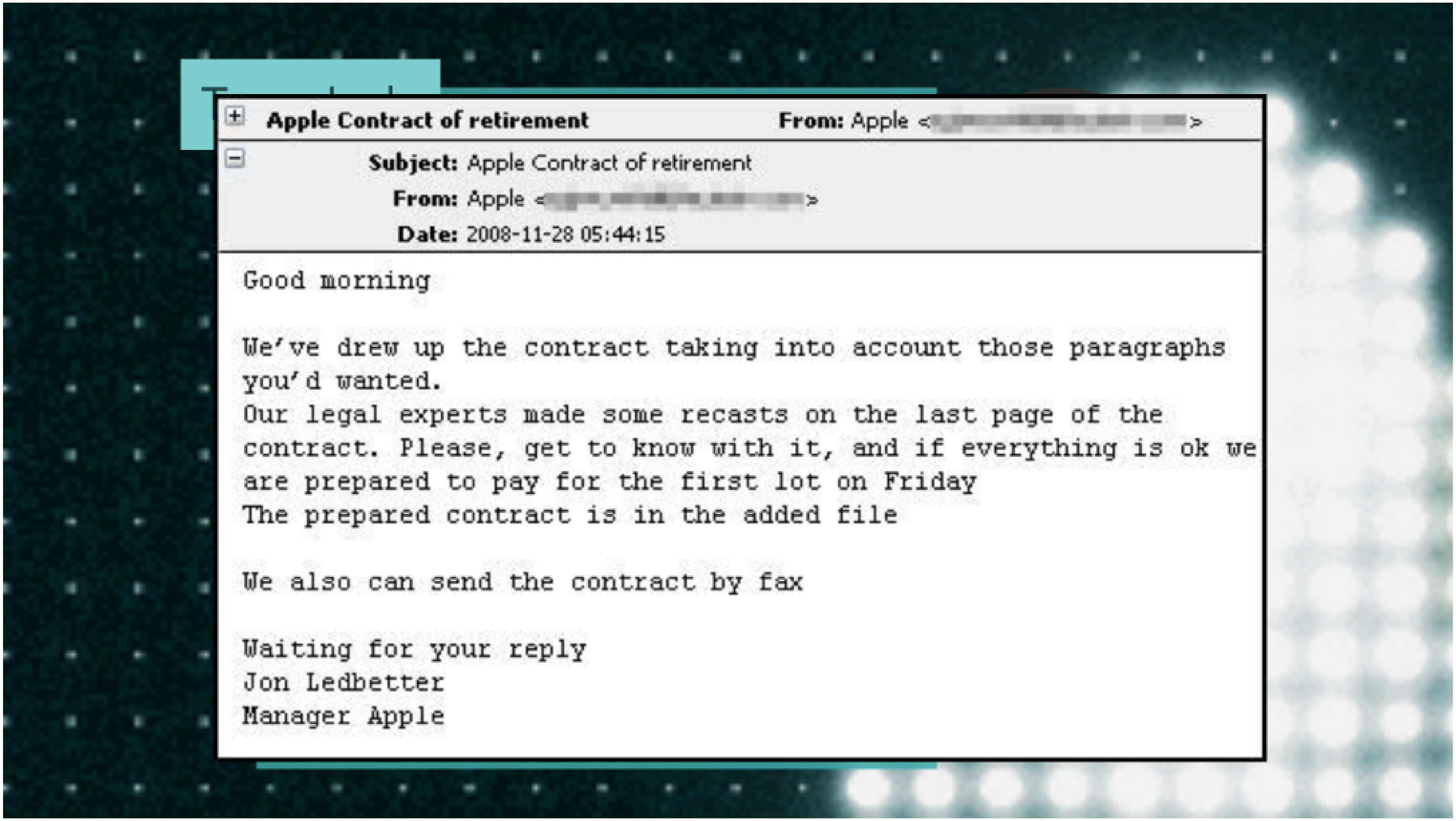


Targeted

Bad actors will use open source information to identify targets.

Once identified, they will uncover target's business email address.

The target then receives Phishing or Trojan emails intended to compromise the target's business email account.



Apple Contract of retirement **From:** Apple <[redacted]>

Subject: Apple Contract of retirement

From: Apple <[redacted]>

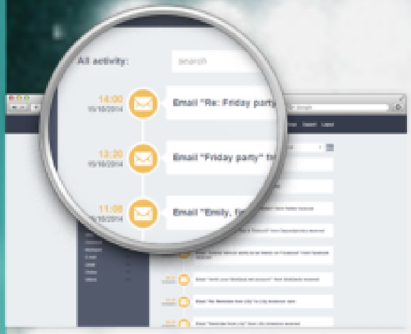
Date: 2008-11-28 05:44:15

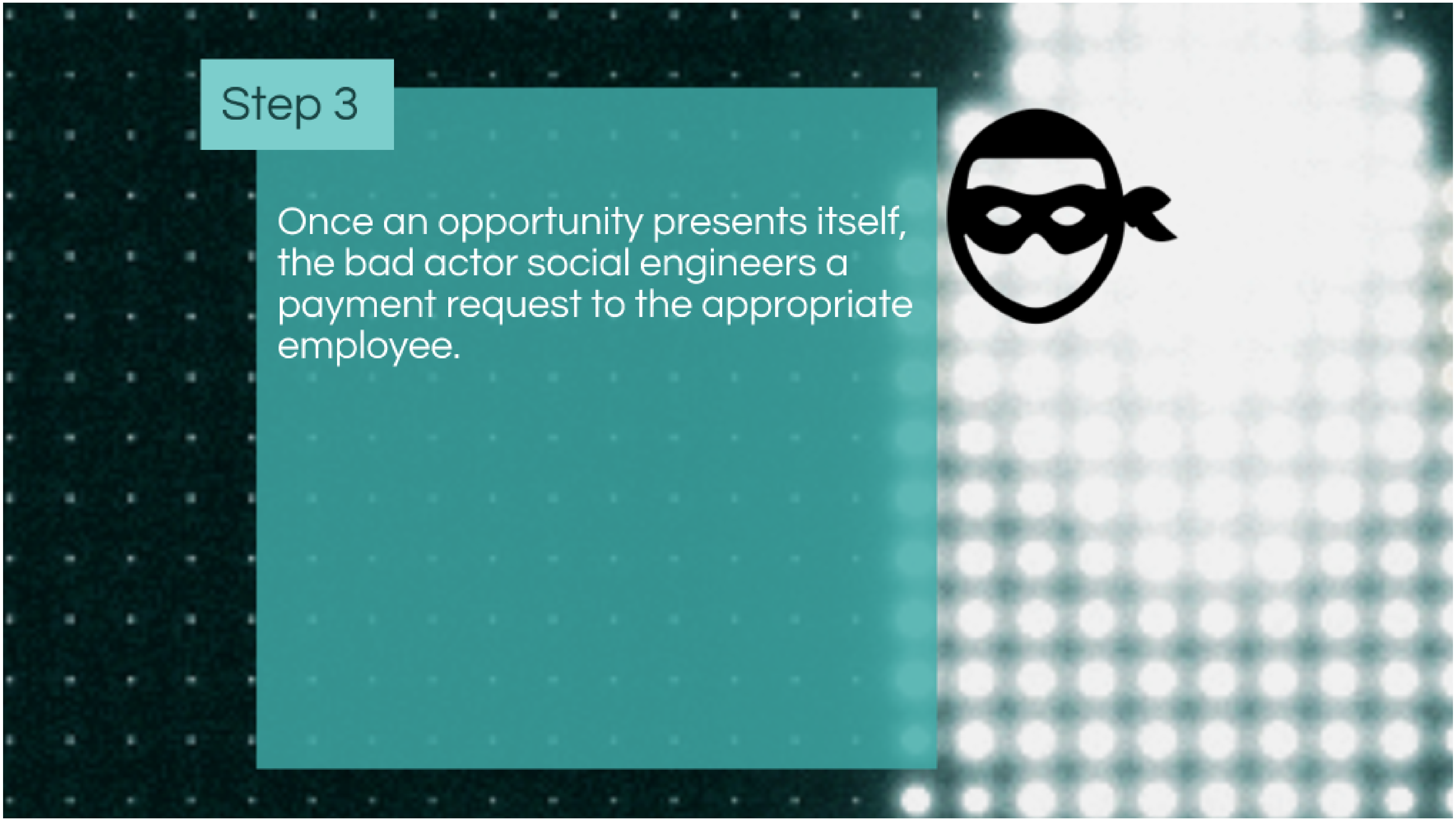
```
Good morning

We’ve drew up the contract taking into account those paragraphs
you’d wanted.
Our legal experts made some recasts on the last page of the
contract. Please, get to know with it, and if everything is ok we
are prepared to pay for the first lot on Friday
The prepared contract is in the added file

We also can send the contract by fax

Waiting for your reply
Jon Ledbetter
Manager Apple
```

Step 2

Once the bad actor has access to email, she will monitor traffic, looking for habit and custom.

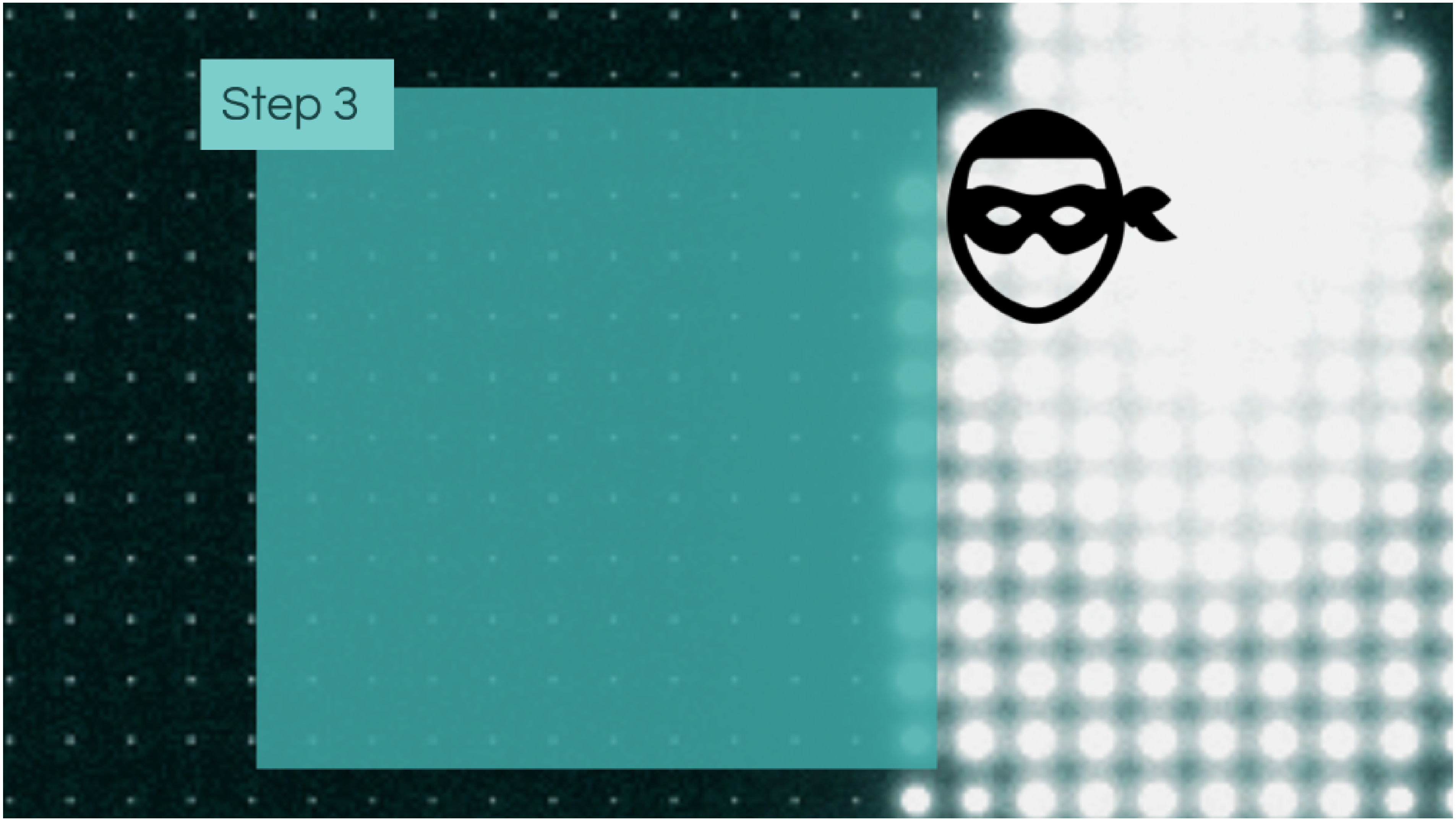
The goal is to learn about accounts payable.





Step 3

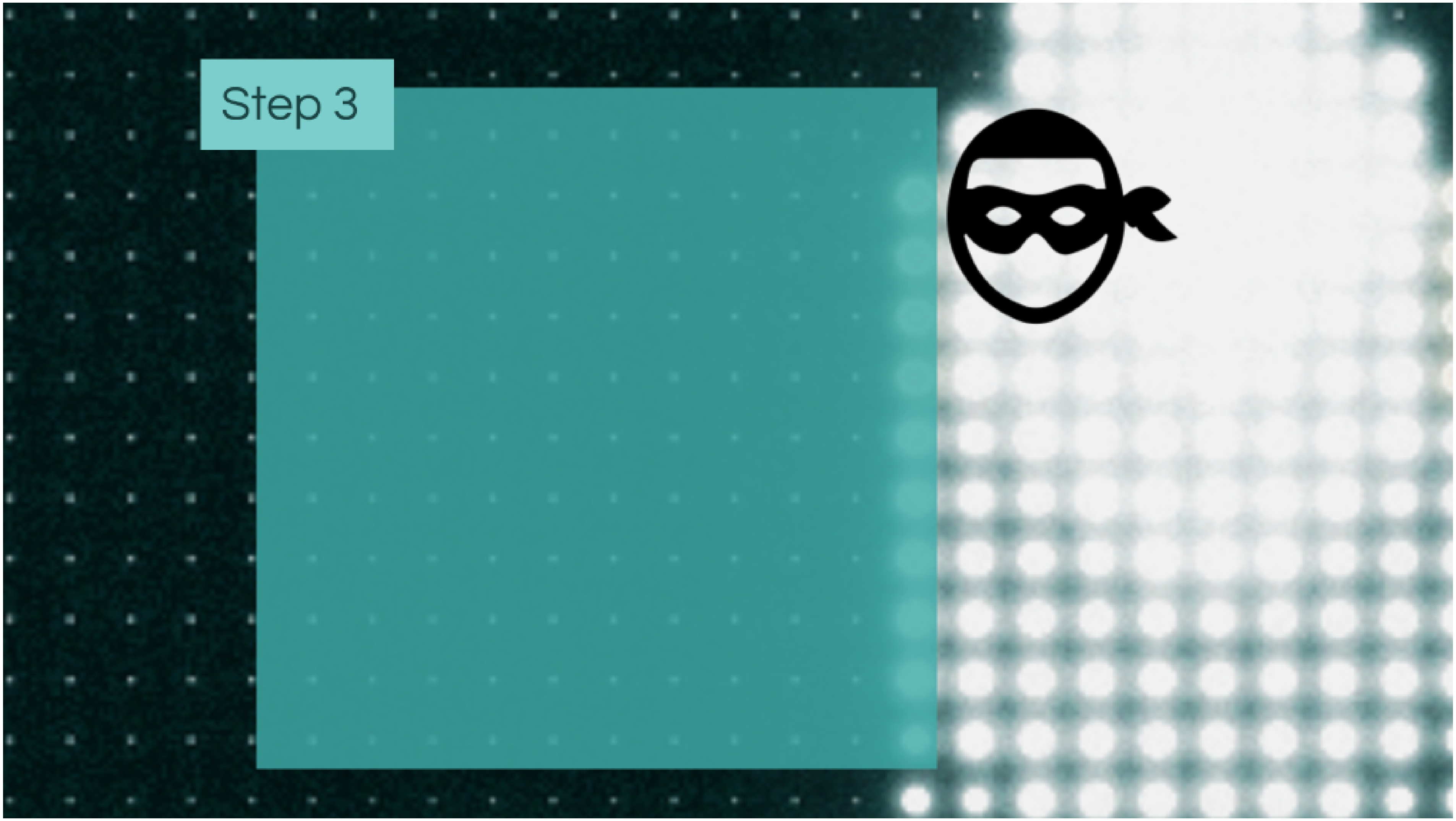
Once an opportunity presents itself, the bad actor social engineers a payment request to the appropriate employee.



Step 3

Step 3

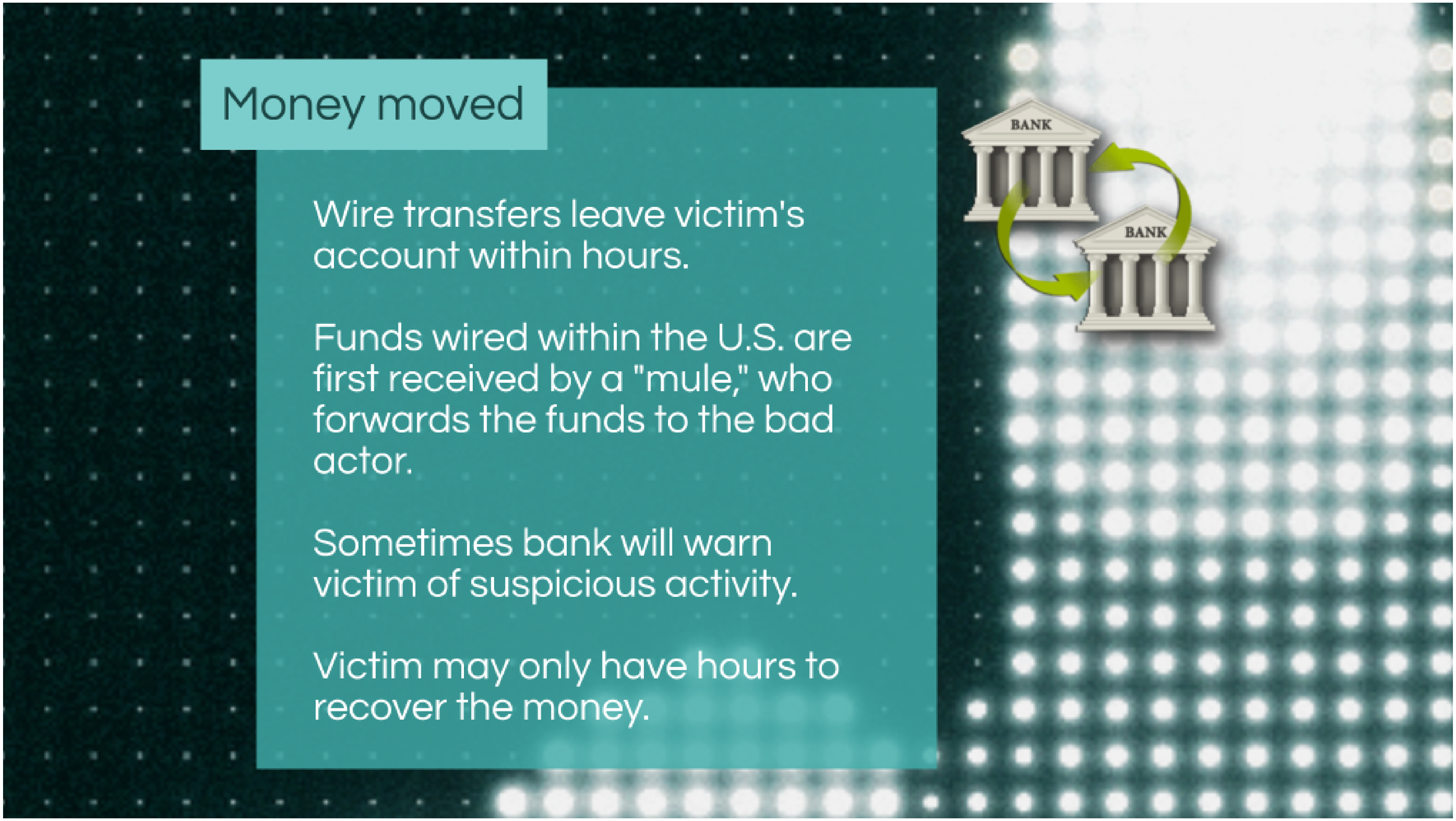
Generally, these requests are made with a sense of urgency, using intelligence gathered during Step 2.



Step 3

Step 3

Payment requests are wire transfers, and can be directed to a U.S. or International bank.



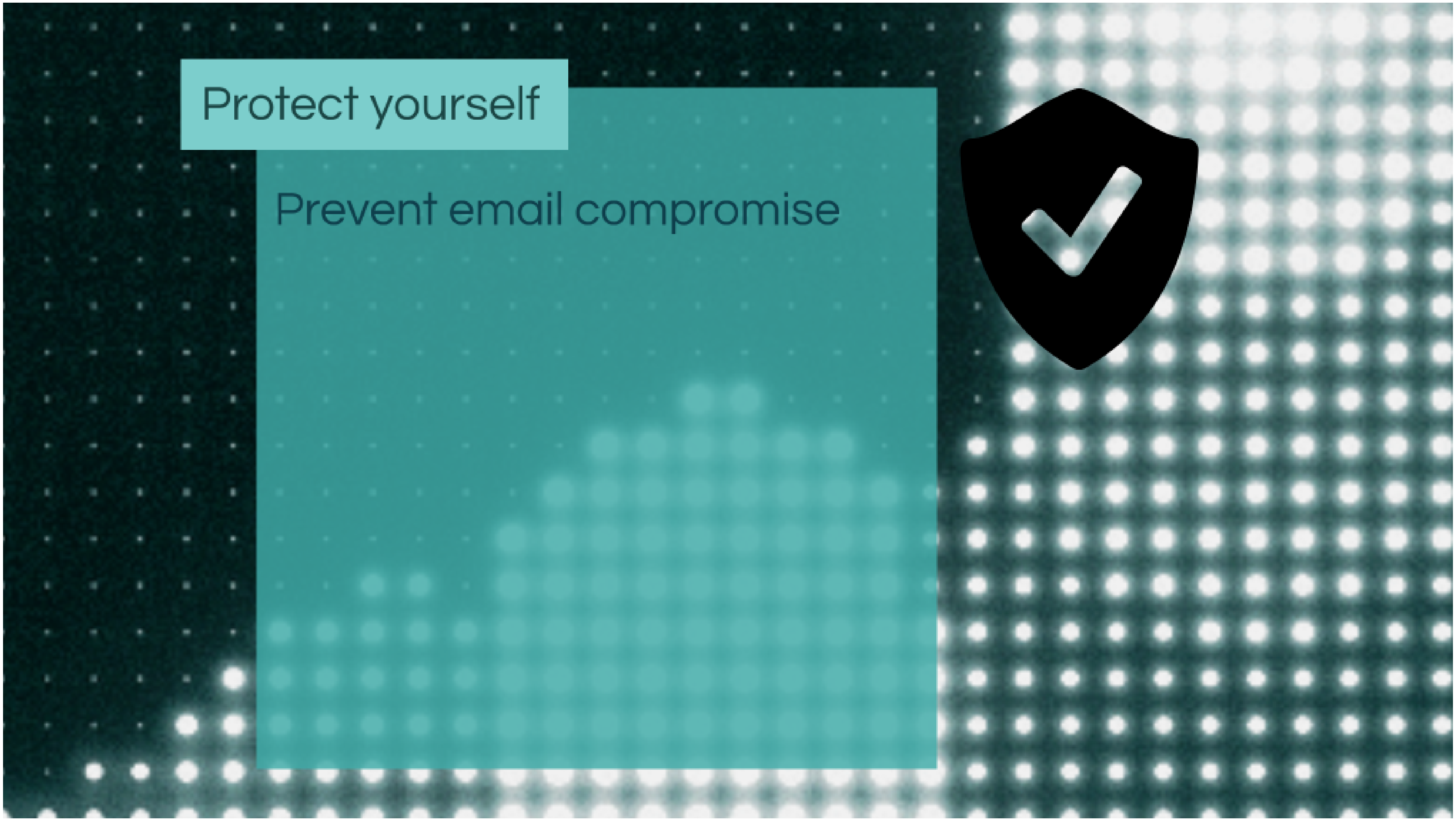
Money moved

Wire transfers leave victim's account within hours.

Funds wired within the U.S. are first received by a "mule," who forwards the funds to the bad actor.

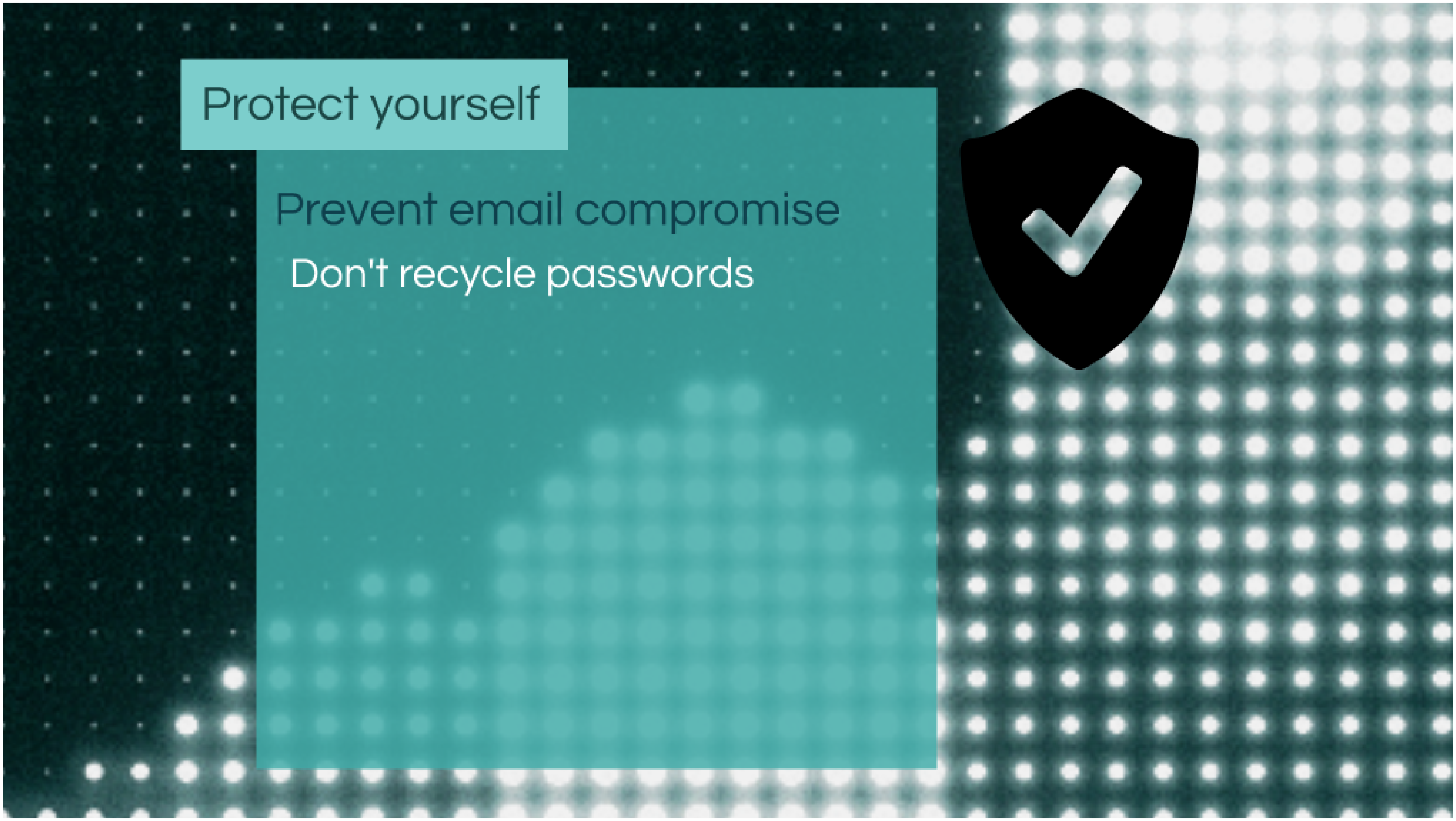
Sometimes bank will warn victim of suspicious activity.

Victim may only have hours to recover the money.



Protect yourself

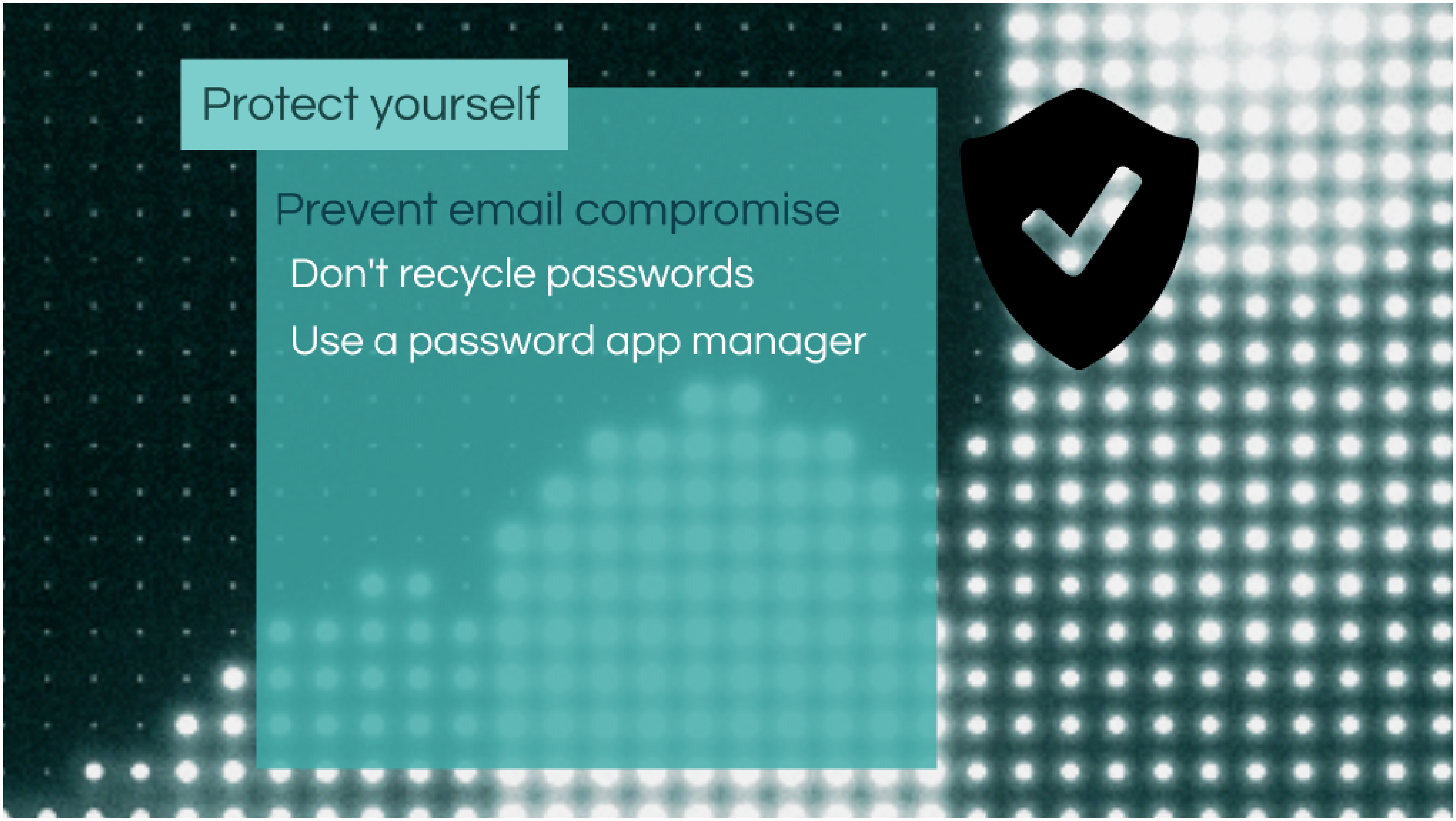
Prevent email compromise



Protect yourself

Prevent email compromise

Don't recycle passwords

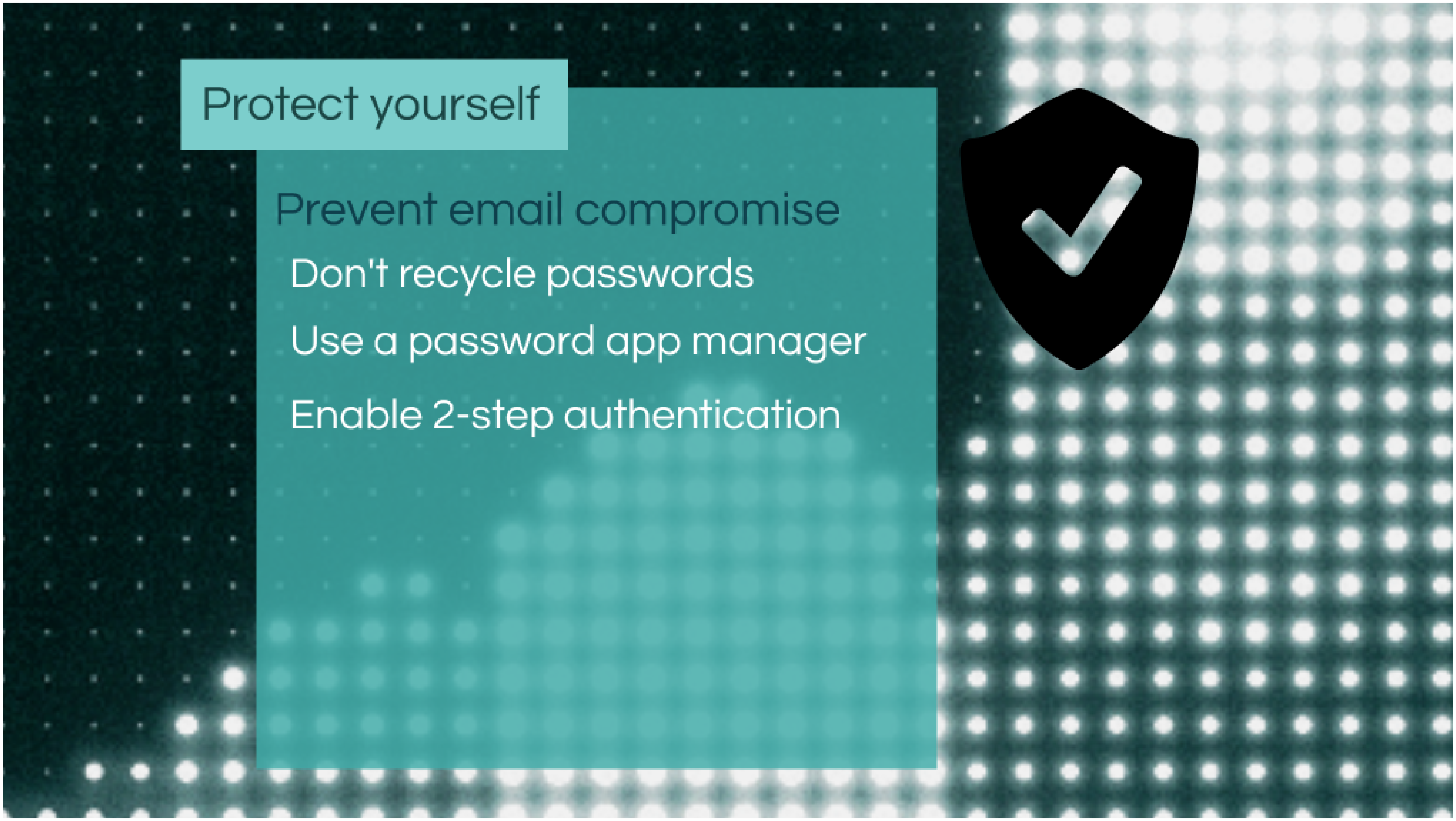


Protect yourself

Prevent email compromise

Don't recycle passwords

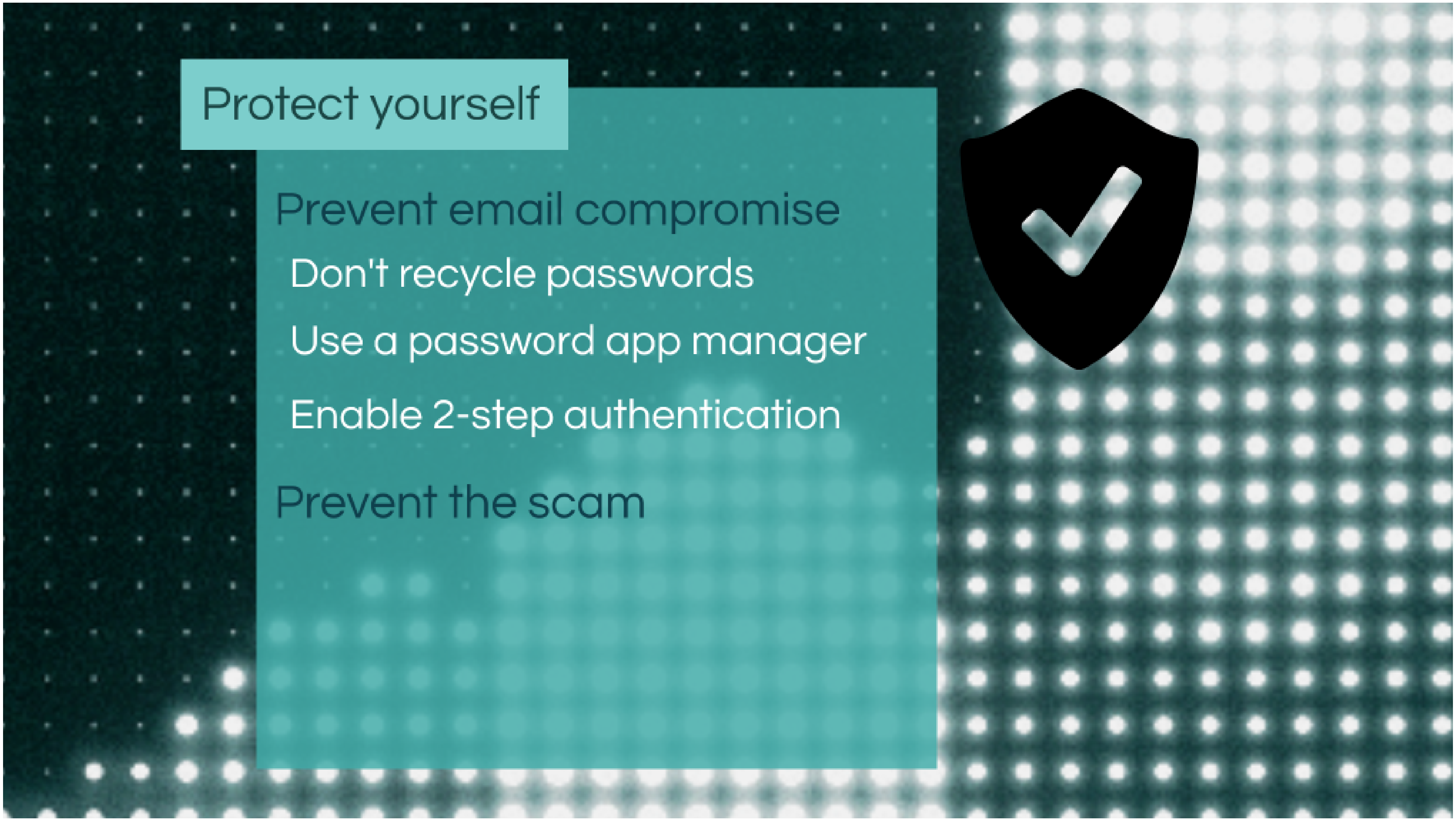
Use a password app manager



Protect yourself

Prevent email compromise

- Don't recycle passwords
- Use a password app manager
- Enable 2-step authentication

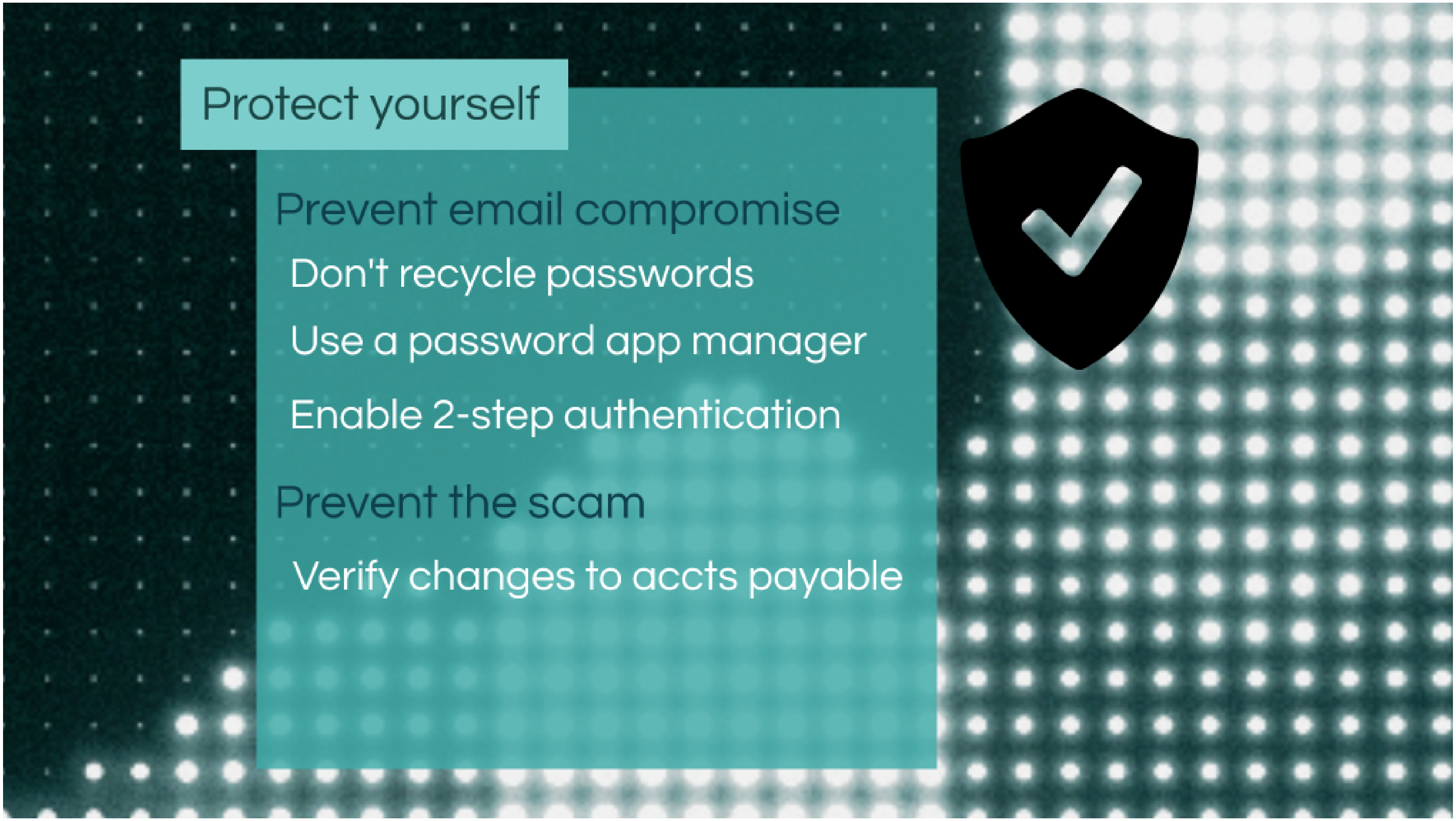


Protect yourself

Prevent email compromise

- Don't recycle passwords
- Use a password app manager
- Enable 2-step authentication

Prevent the scam



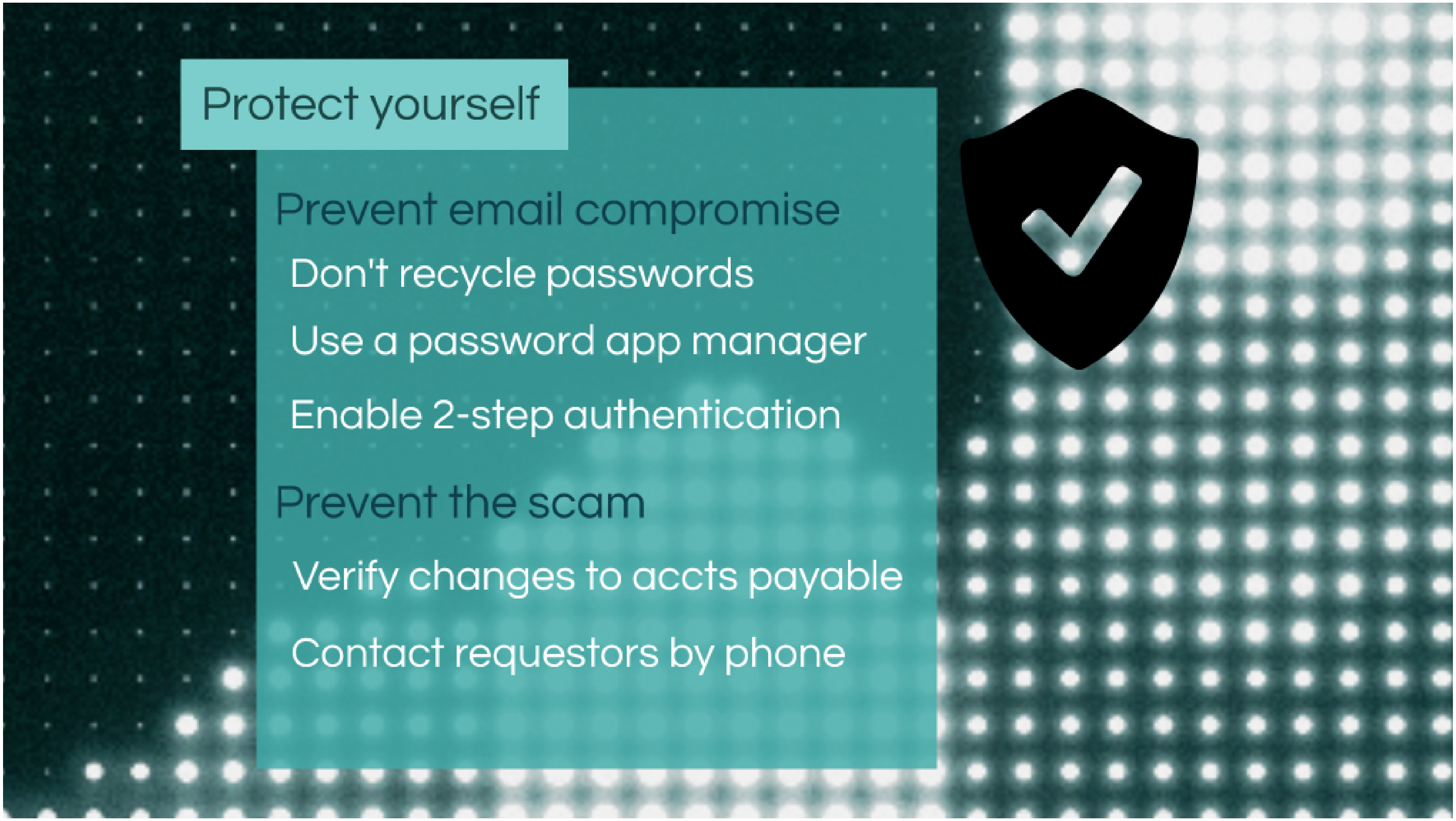
Protect yourself

Prevent email compromise

- Don't recycle passwords
- Use a password app manager
- Enable 2-step authentication

Prevent the scam

- Verify changes to accts payable



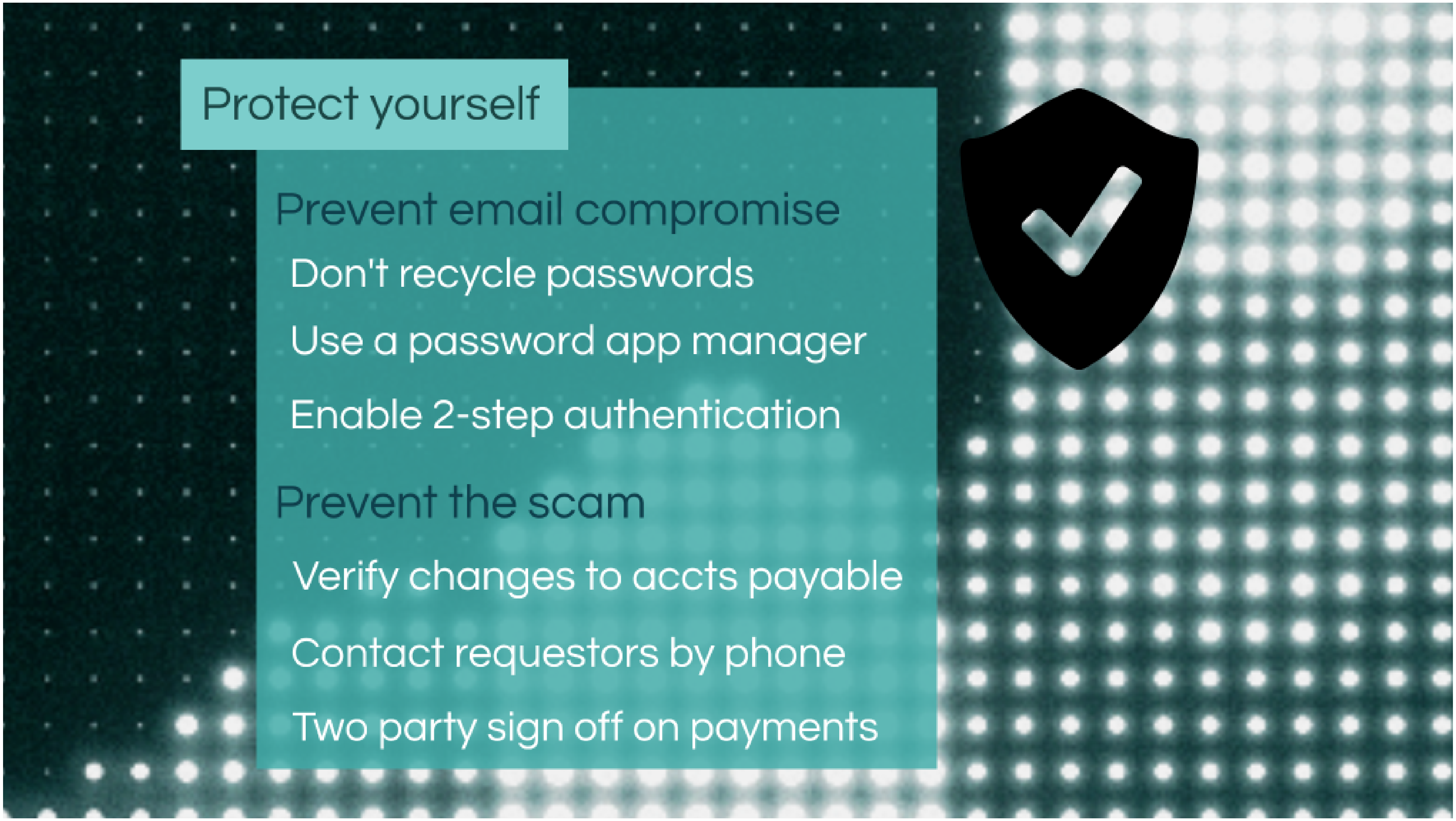
Protect yourself

Prevent email compromise

- Don't recycle passwords
- Use a password app manager
- Enable 2-step authentication

Prevent the scam

- Verify changes to accts payable
- Contact requestors by phone



Protect yourself

Prevent email compromise

- Don't recycle passwords
- Use a password app manager
- Enable 2-step authentication

Prevent the scam

- Verify changes to accts payable
- Contact requestors by phone
- Two party sign off on payments

GLOBAL THREATS TO LOCAL BUSINESS: EMAIL COMPROMISE & RANSOMWARE

What is the Threat?

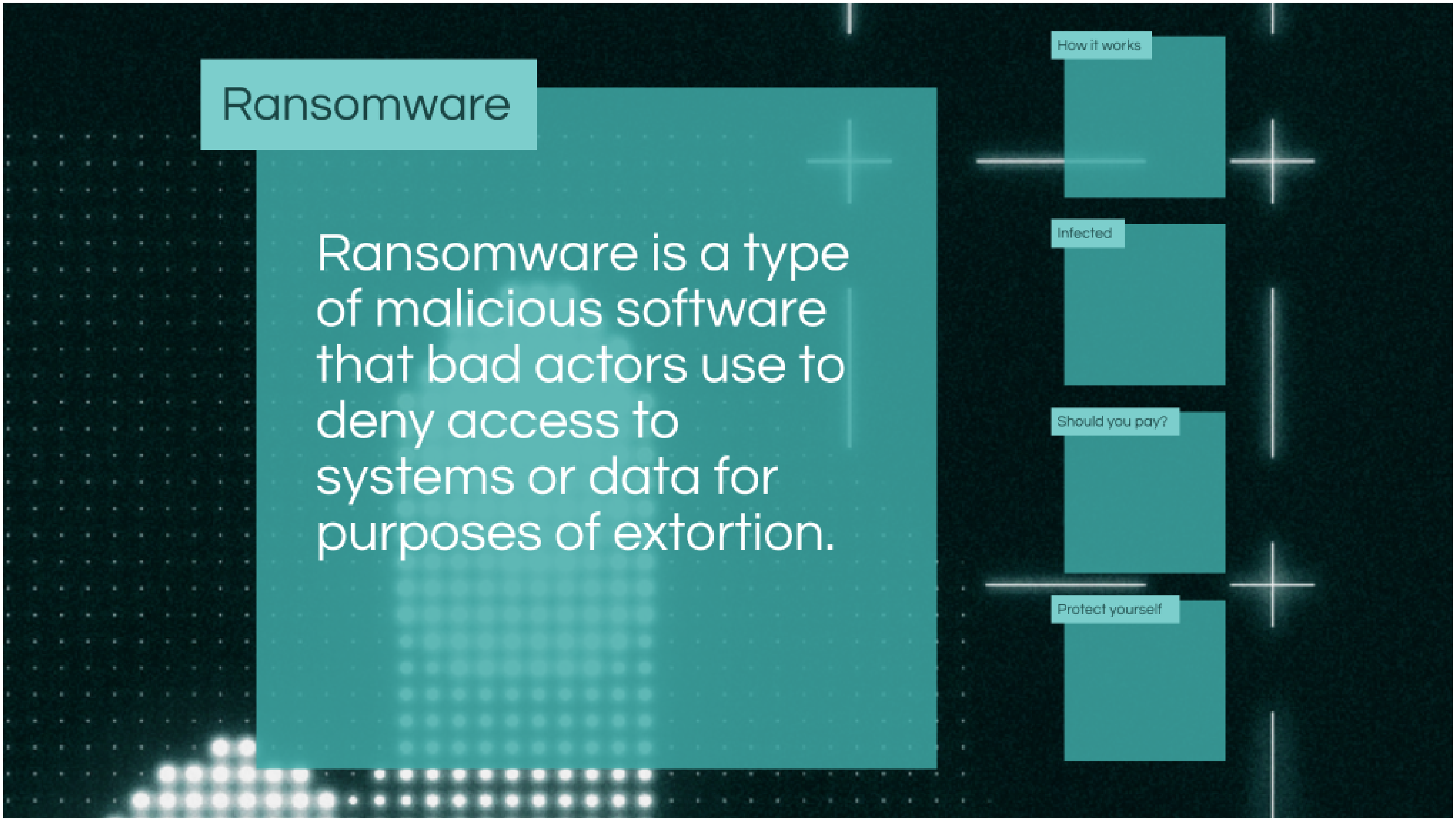
Overview

Business Email Compromise

Ransomware

Conclusion

A public service by
The San Mateo County
District Attorney's Office



Ransomware

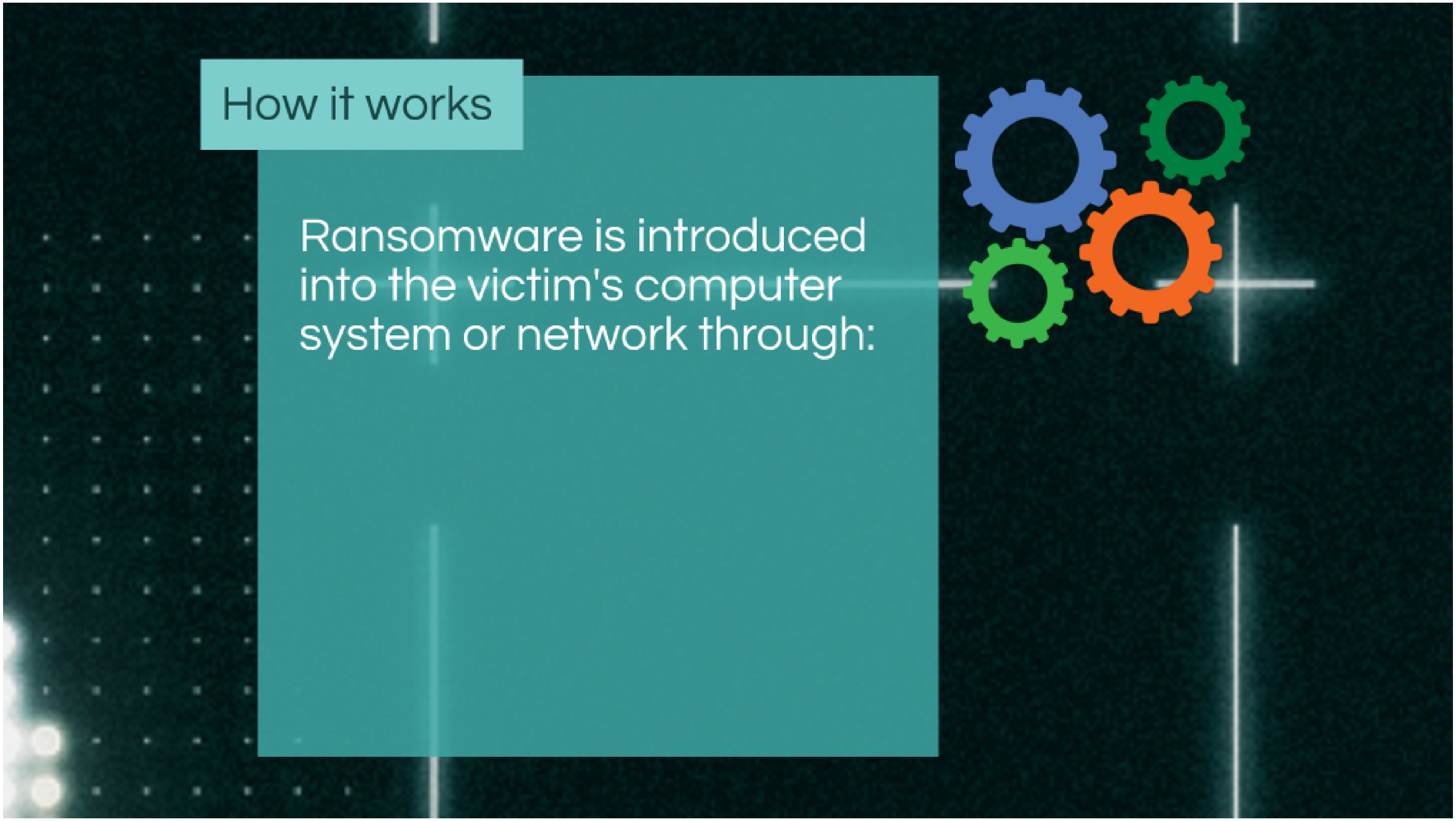
Ransomware is a type of malicious software that bad actors use to deny access to systems or data for purposes of extortion.

How it works

Infected

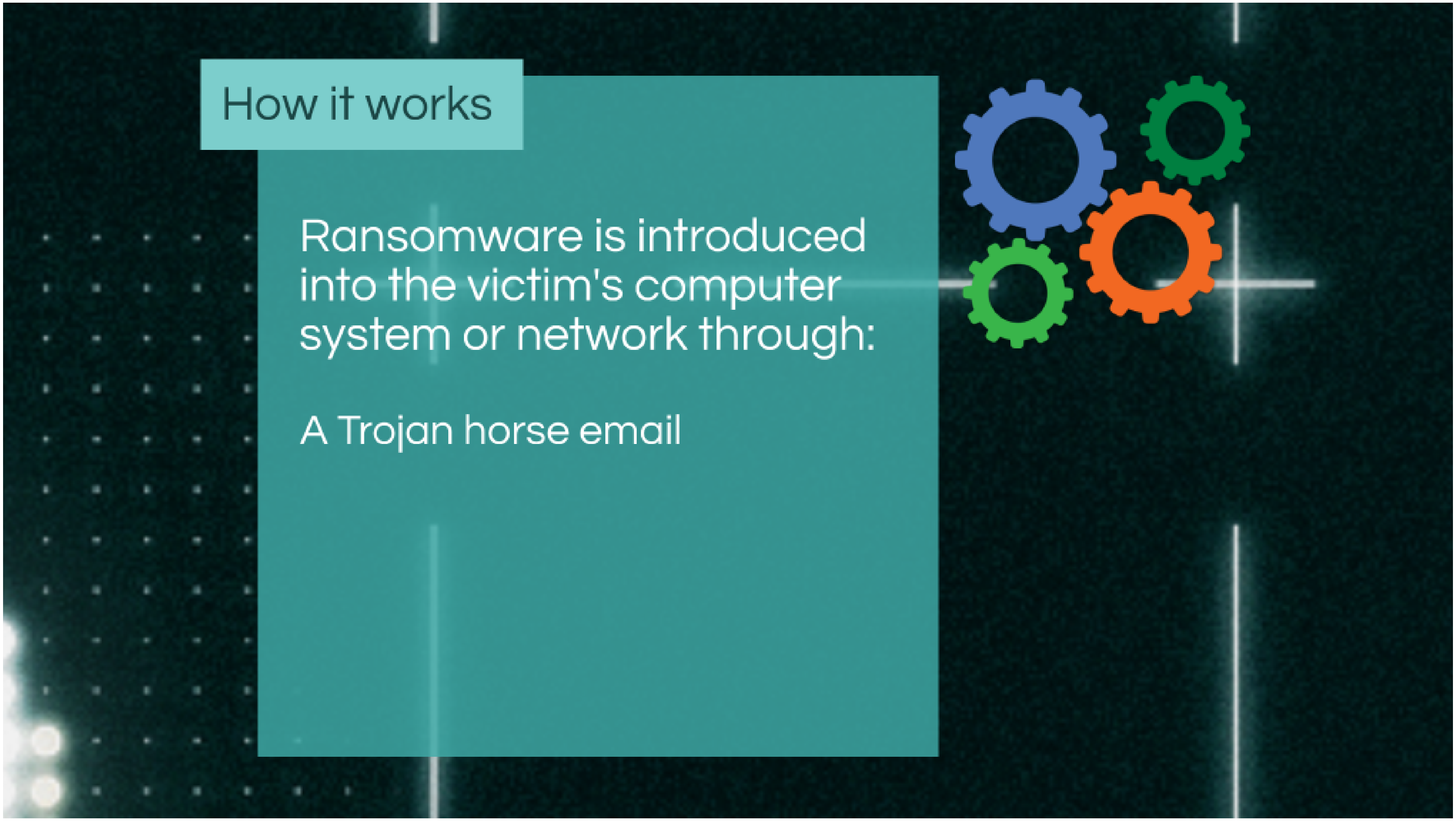
Should you pay?

Protect yourself



How it works

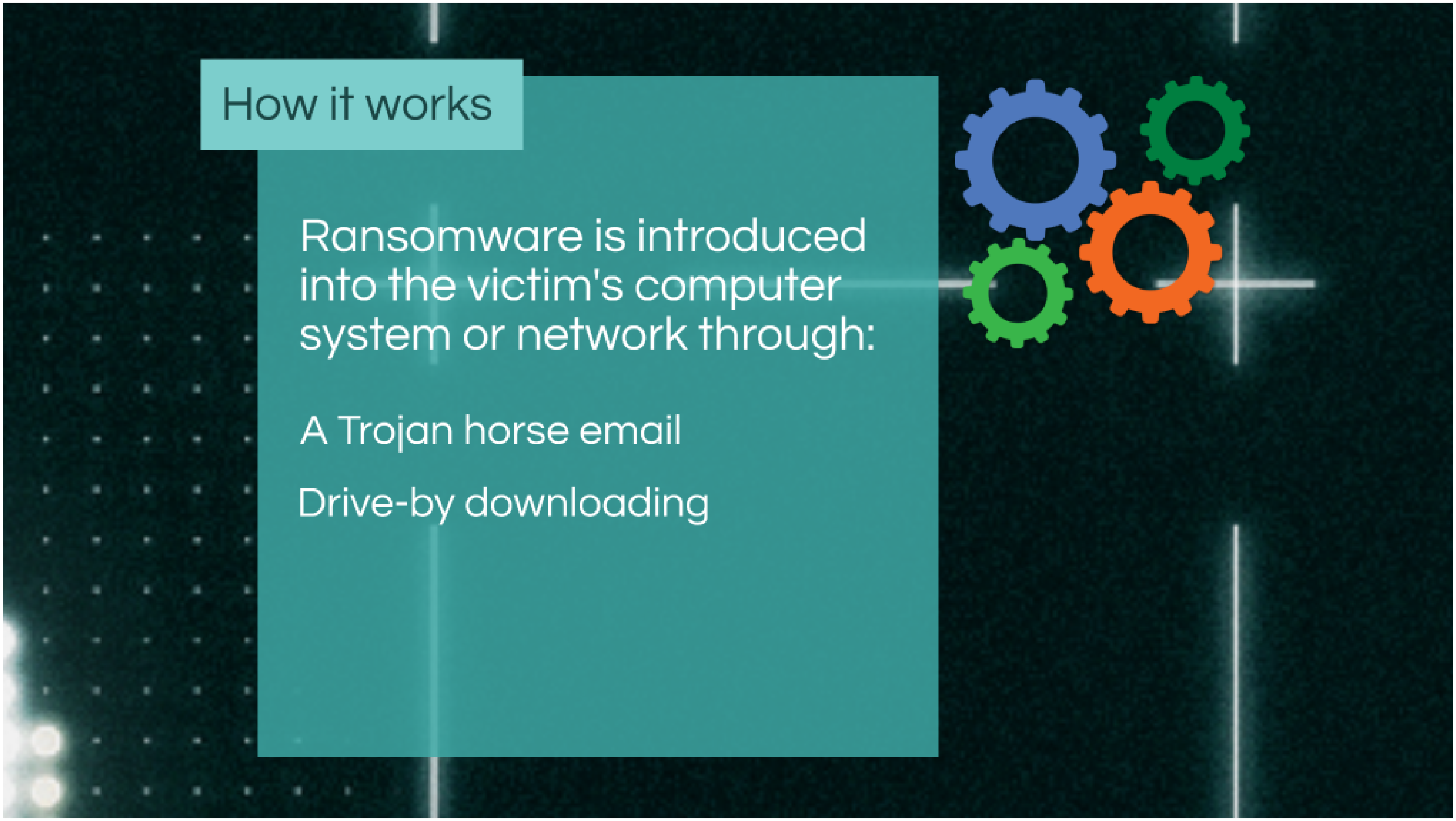
Ransomware is introduced into the victim's computer system or network through:



How it works

Ransomware is introduced into the victim's computer system or network through:

A Trojan horse email

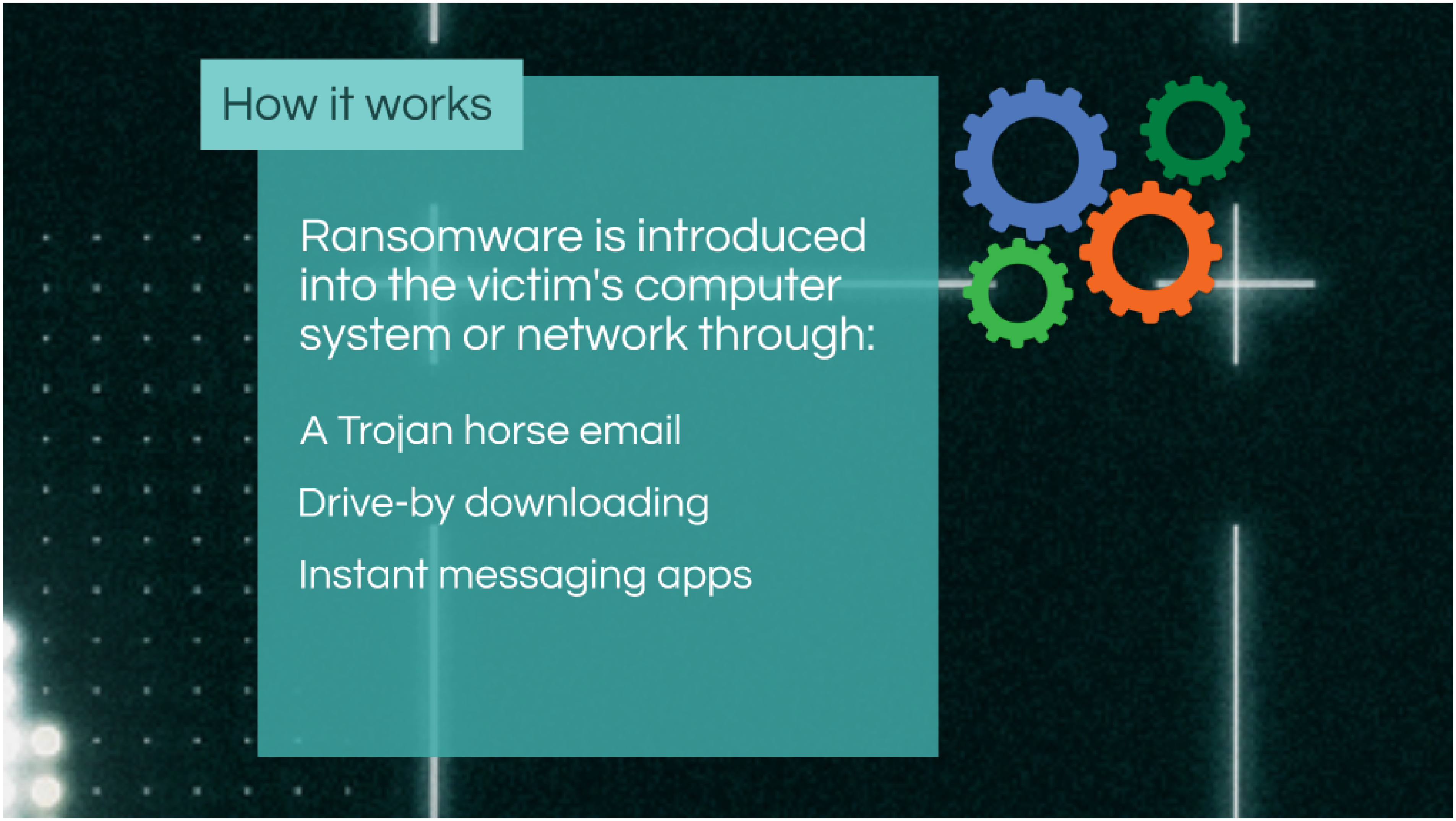


How it works

Ransomware is introduced into the victim's computer system or network through:

A Trojan horse email

Drive-by downloading



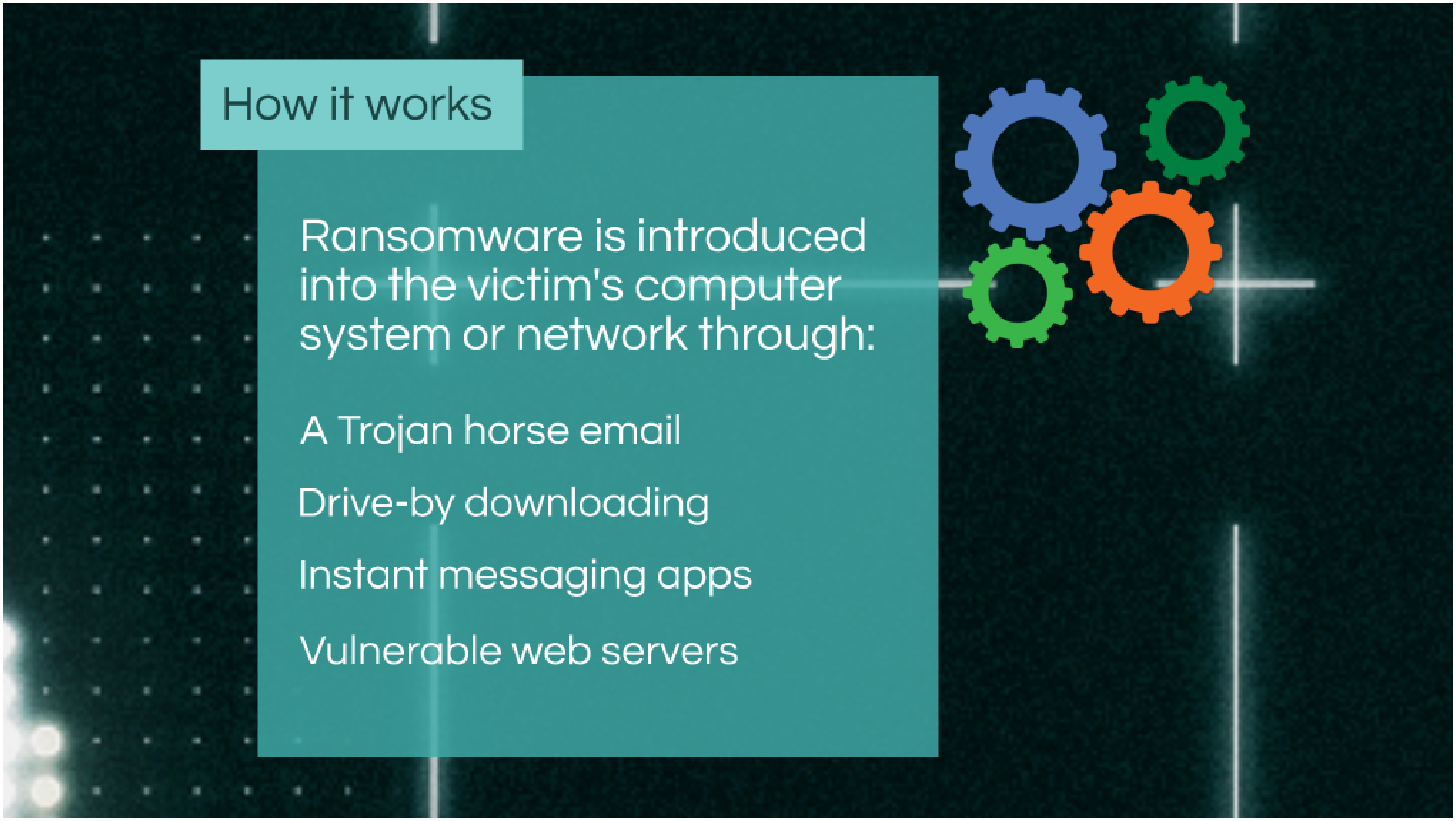
How it works

Ransomware is introduced into the victim's computer system or network through:

A Trojan horse email

Drive-by downloading

Instant messaging apps



How it works

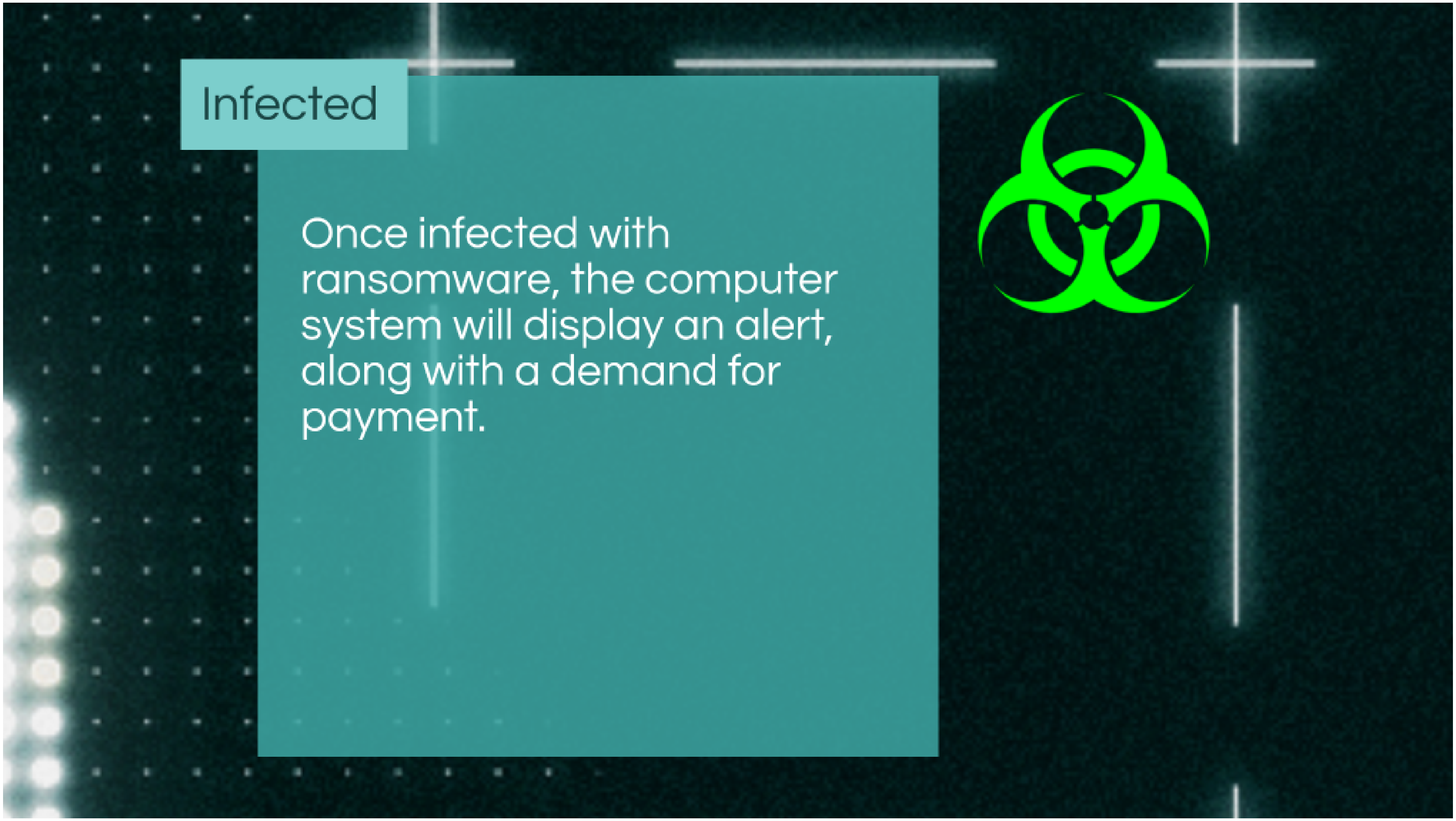
Ransomware is introduced into the victim's computer system or network through:

A Trojan horse email

Drive-by downloading

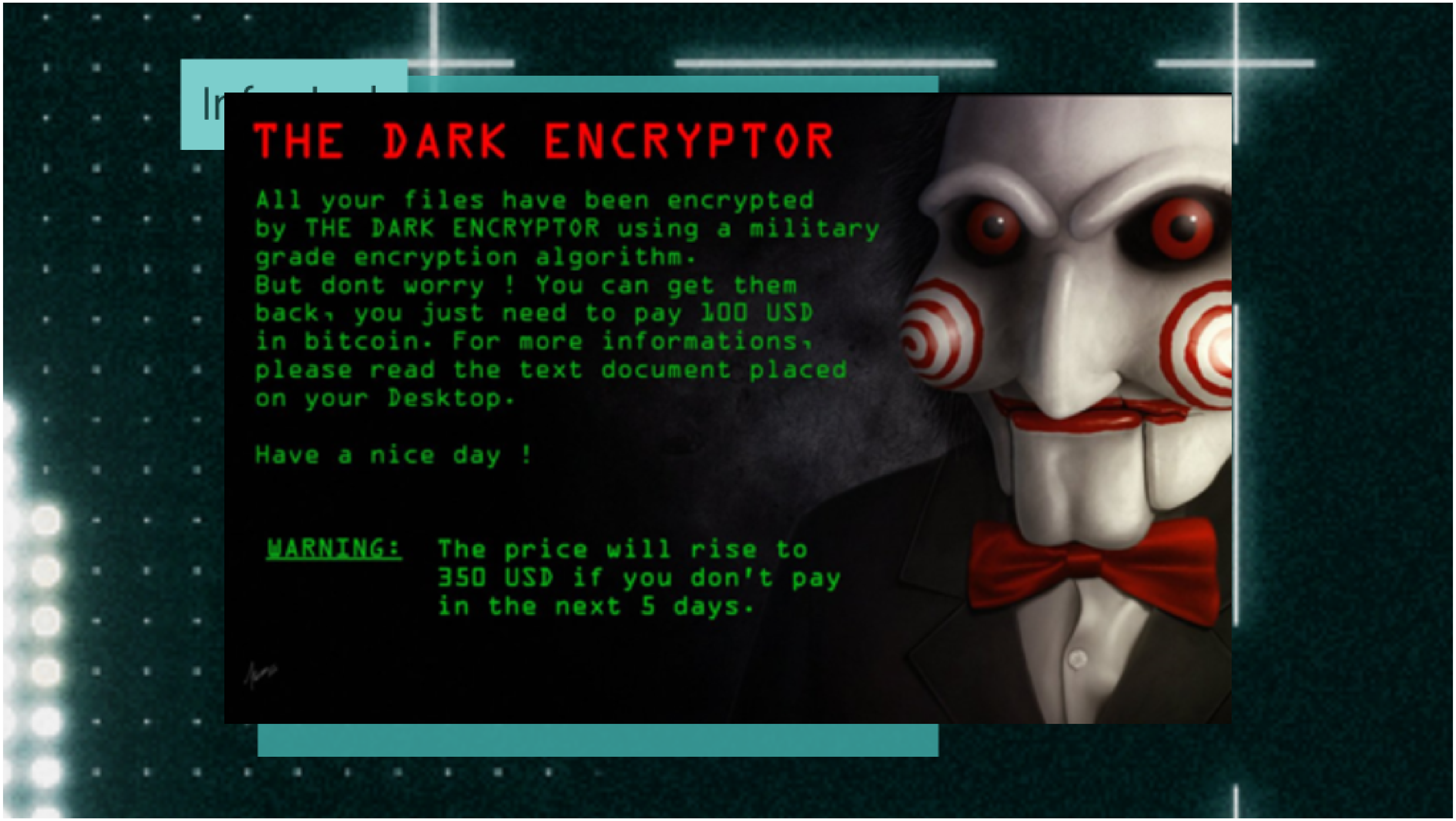
Instant messaging apps

Vulnerable web servers



Infected

Once infected with ransomware, the computer system will display an alert, along with a demand for payment.

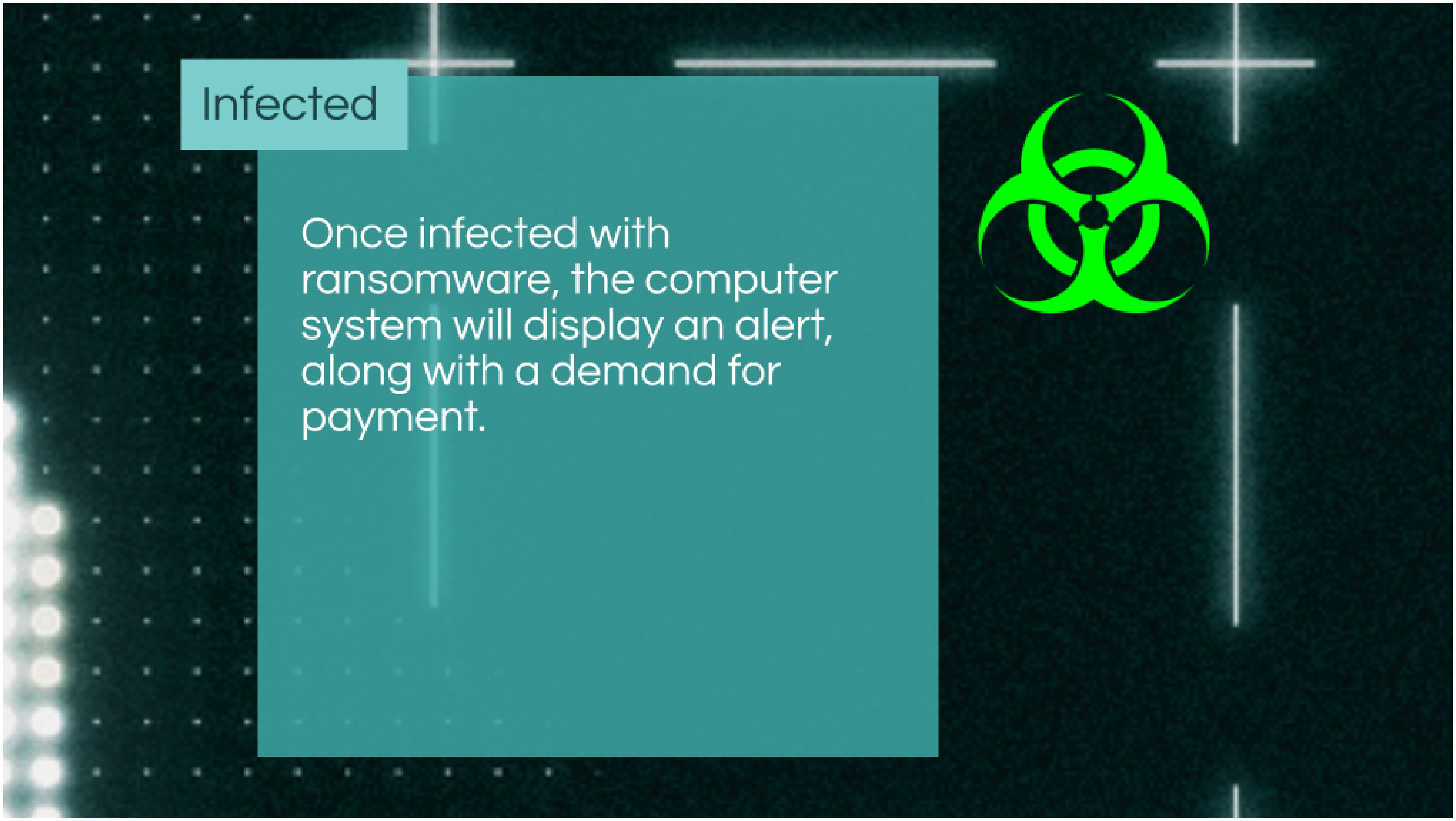


THE DARK ENCRYPTOR

All your files have been encrypted by THE DARK ENCRYPTOR using a military grade encryption algorithm.
But dont worry ! You can get them back, you just need to pay 100 USD in bitcoin. For more informations, please read the text document placed on your Desktop.

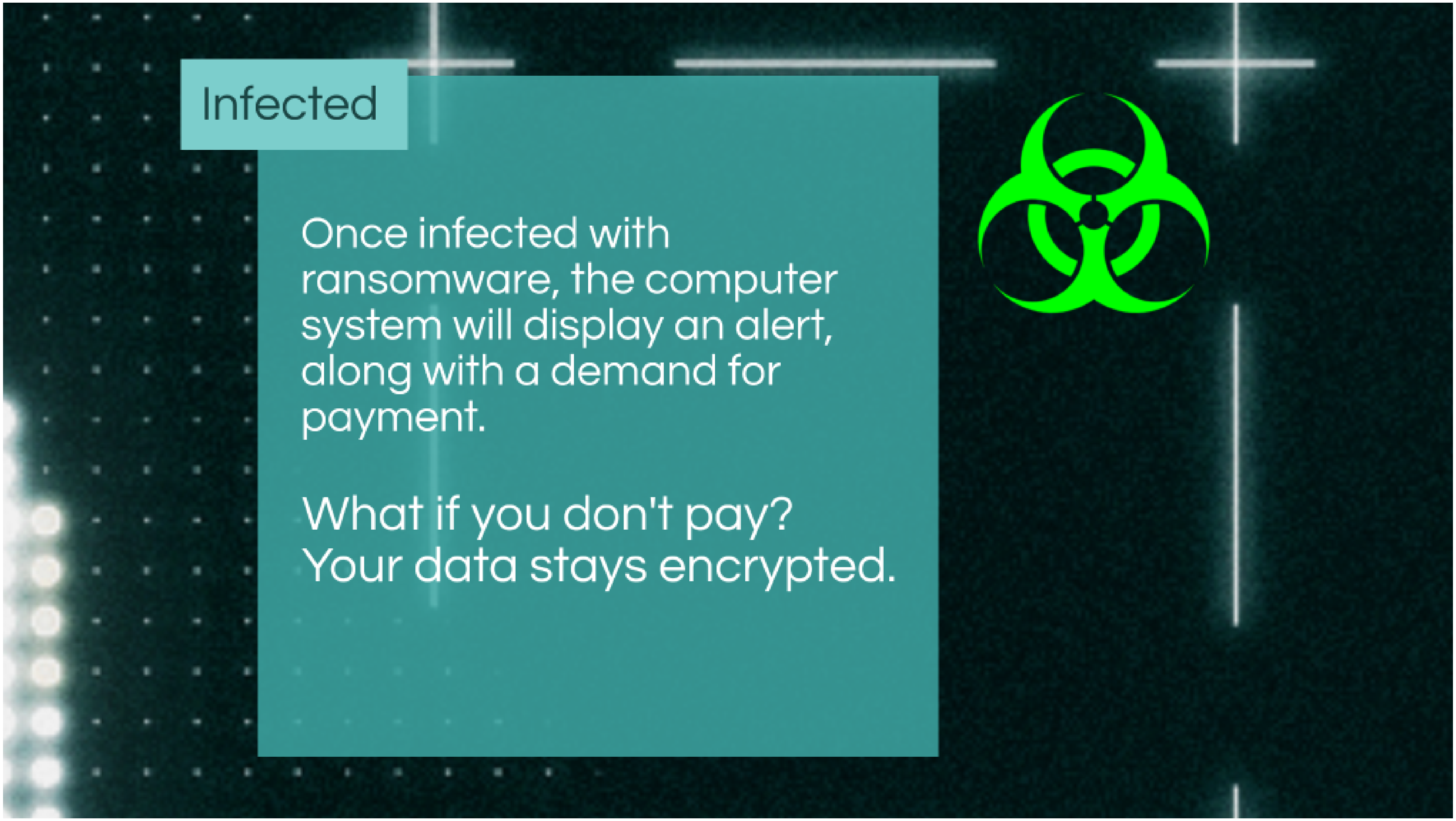
Have a nice day !

WARNING: The price will rise to 350 USD if you don't pay in the next 5 days.



Infected

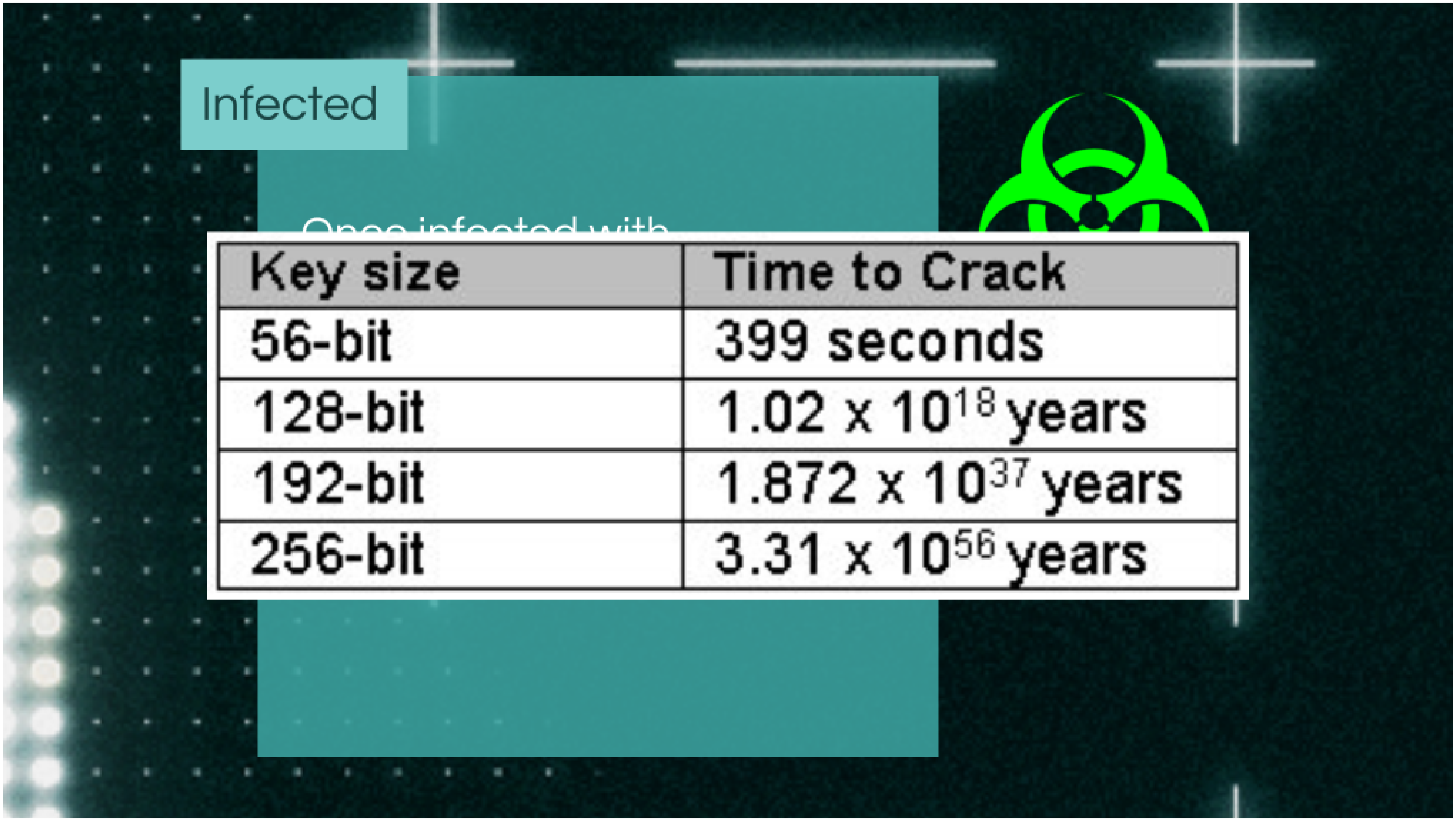
Once infected with ransomware, the computer system will display an alert, along with a demand for payment.



Infected

Once infected with ransomware, the computer system will display an alert, along with a demand for payment.

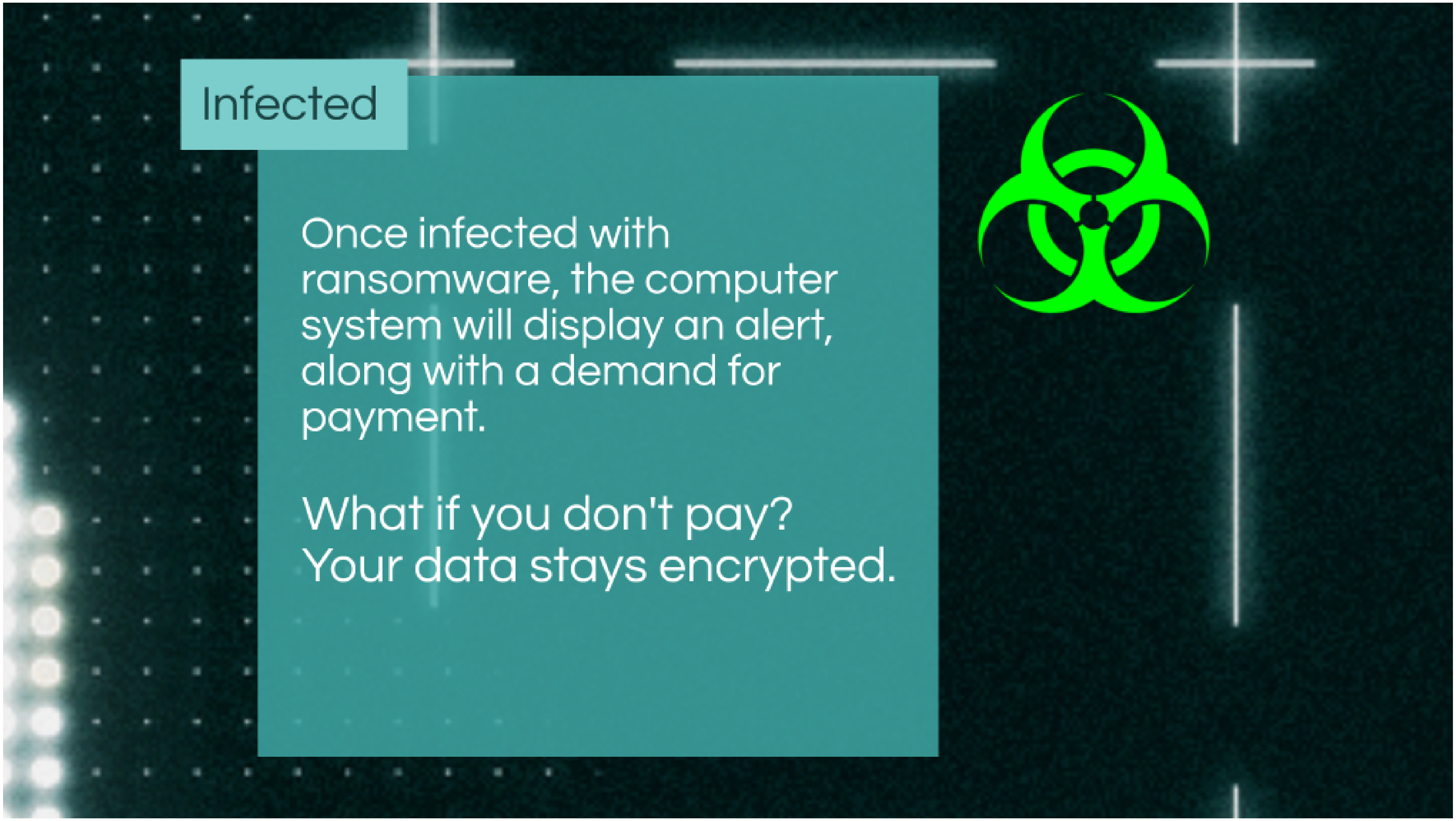
What if you don't pay? Your data stays encrypted.



Infected

Once infected with

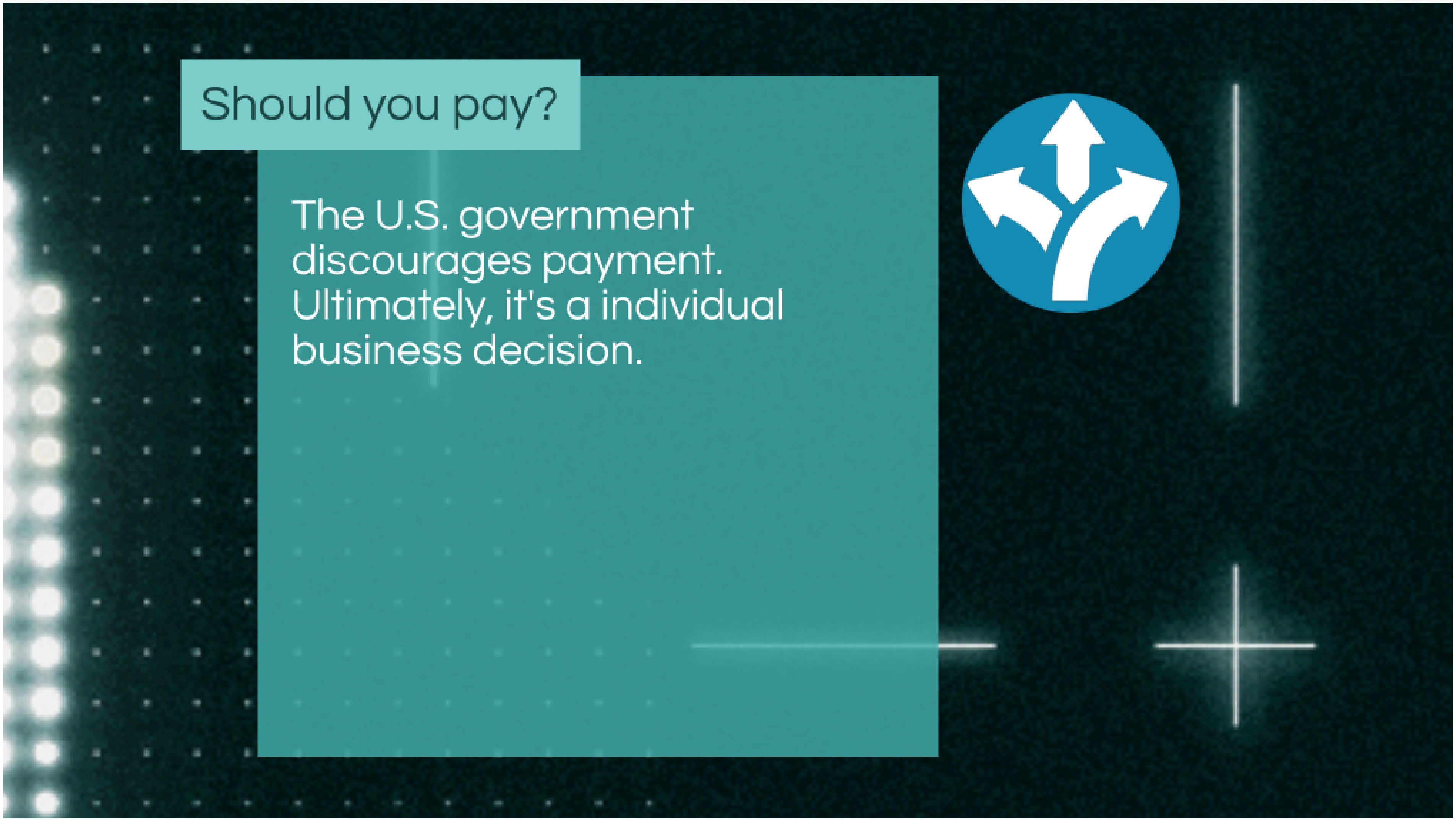
Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02 x 10^{18} years
192-bit	1.872 x 10^{37} years
256-bit	3.31 x 10^{56} years



Infected

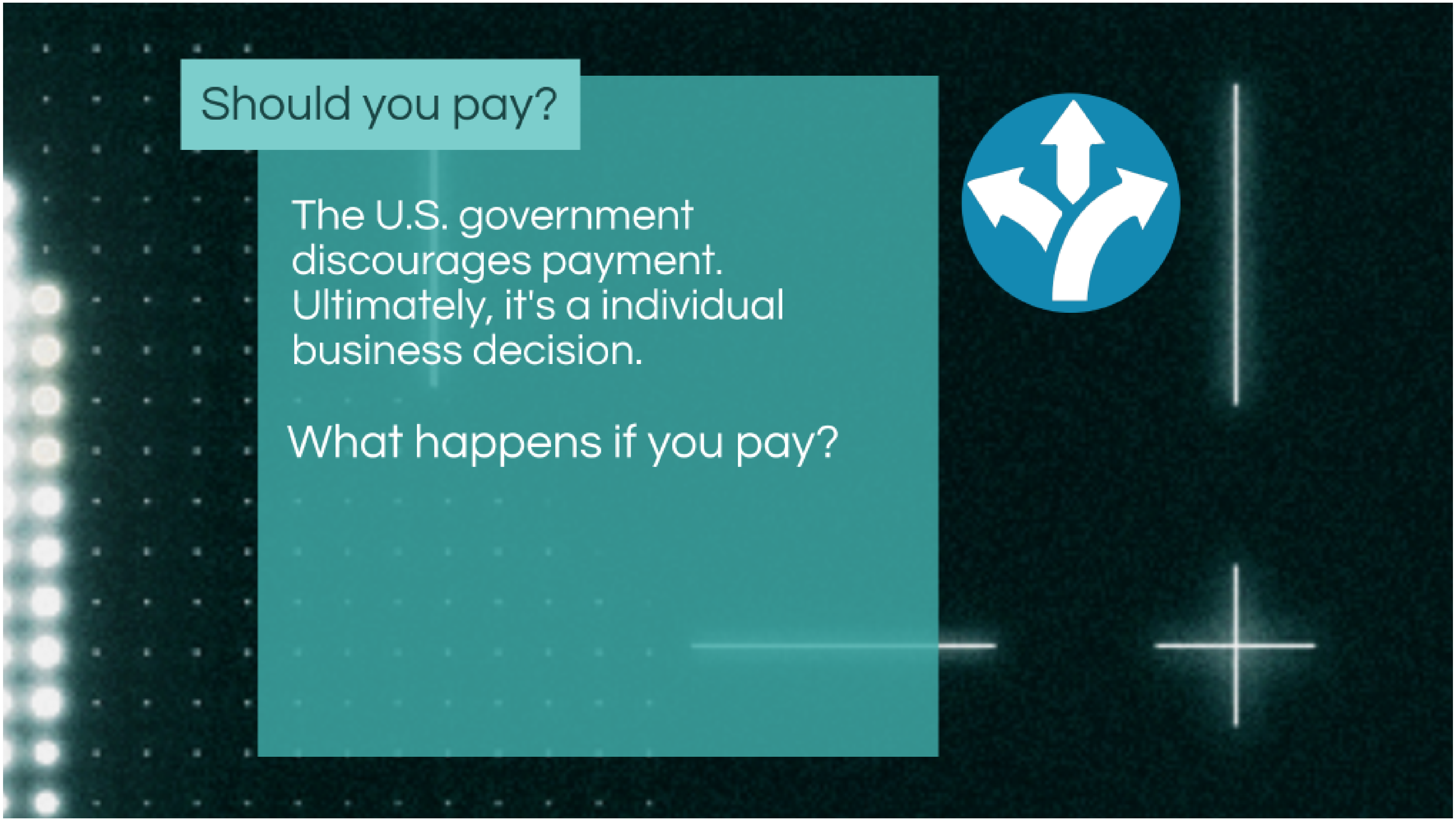
Once infected with ransomware, the computer system will display an alert, along with a demand for payment.

What if you don't pay? Your data stays encrypted.



Should you pay?

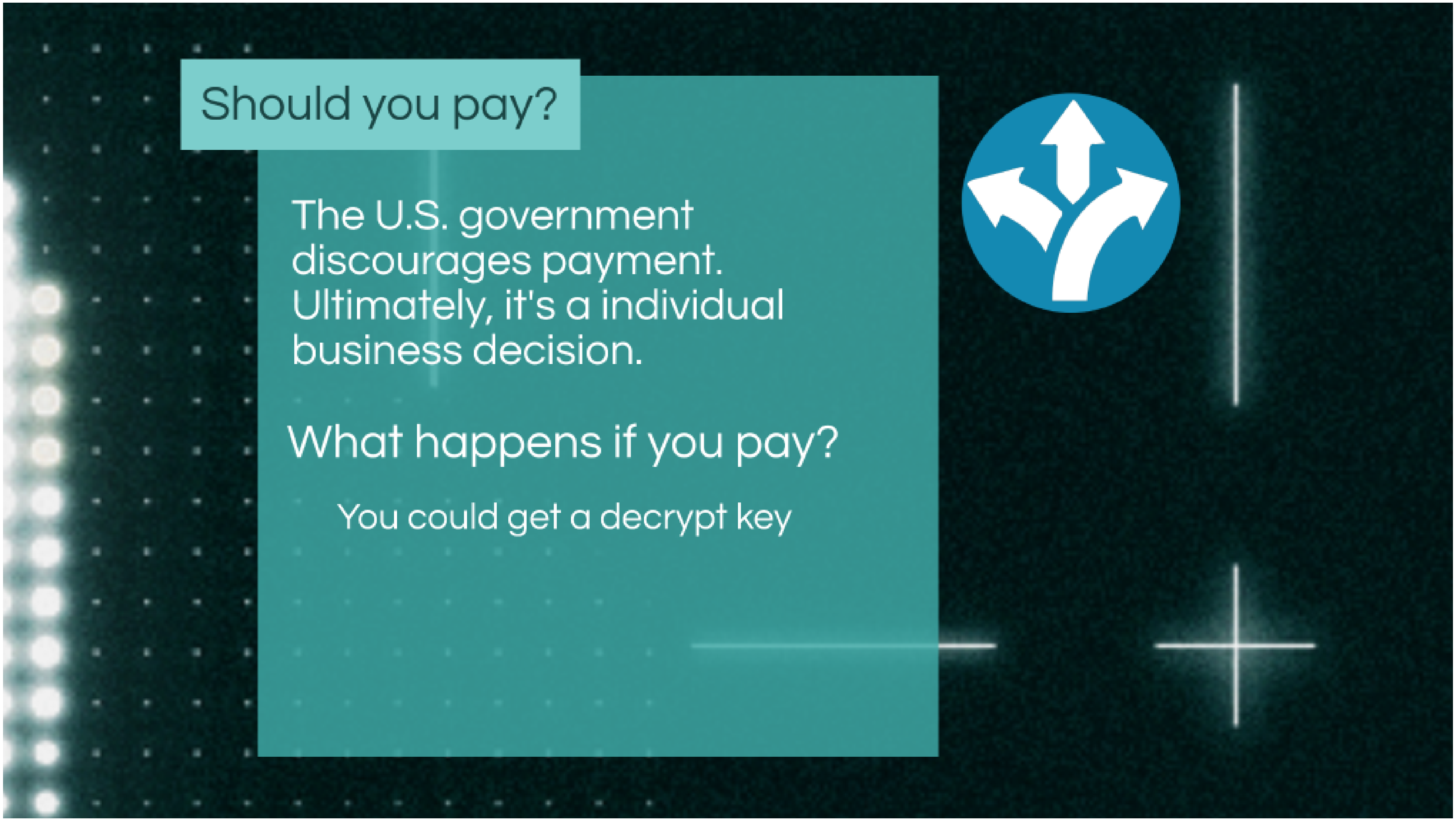
The U.S. government discourages payment. Ultimately, it's a individual business decision.



Should you pay?

The U.S. government discourages payment. Ultimately, it's a individual business decision.

What happens if you pay?

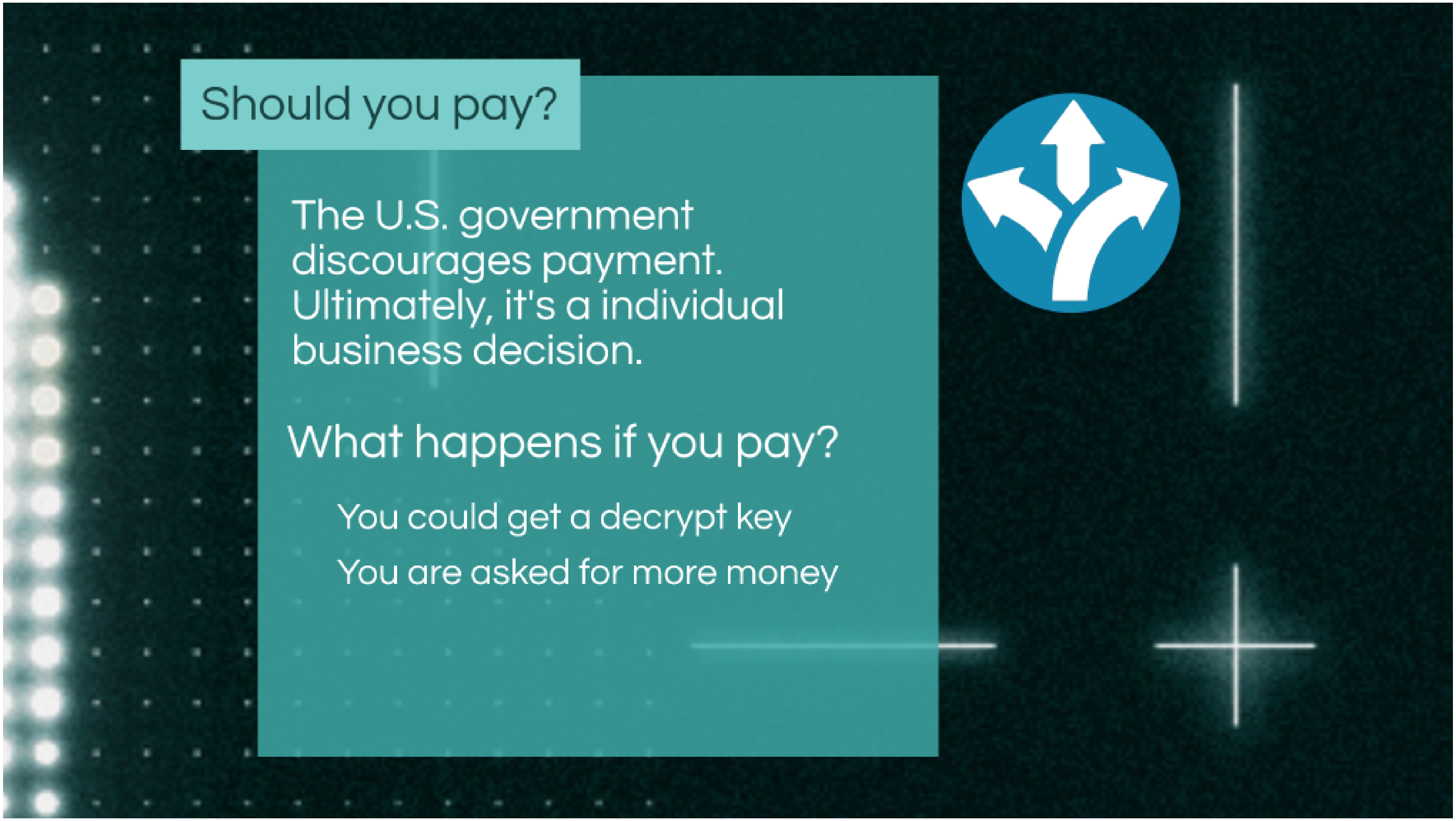


Should you pay?

The U.S. government discourages payment. Ultimately, it's a individual business decision.

What happens if you pay?

You could get a decrypt key

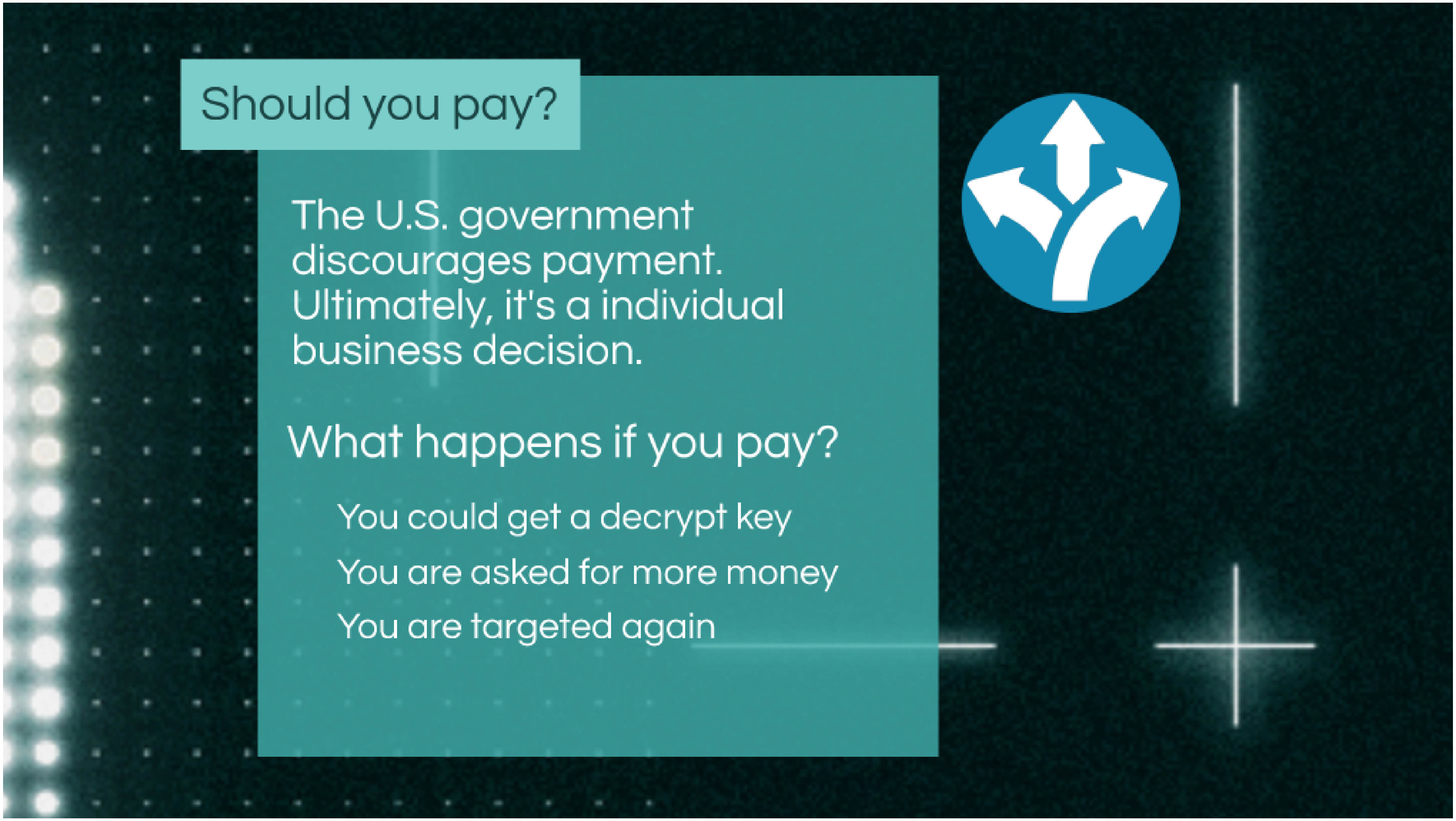


Should you pay?

The U.S. government discourages payment. Ultimately, it's a individual business decision.

What happens if you pay?

- You could get a decrypt key
- You are asked for more money

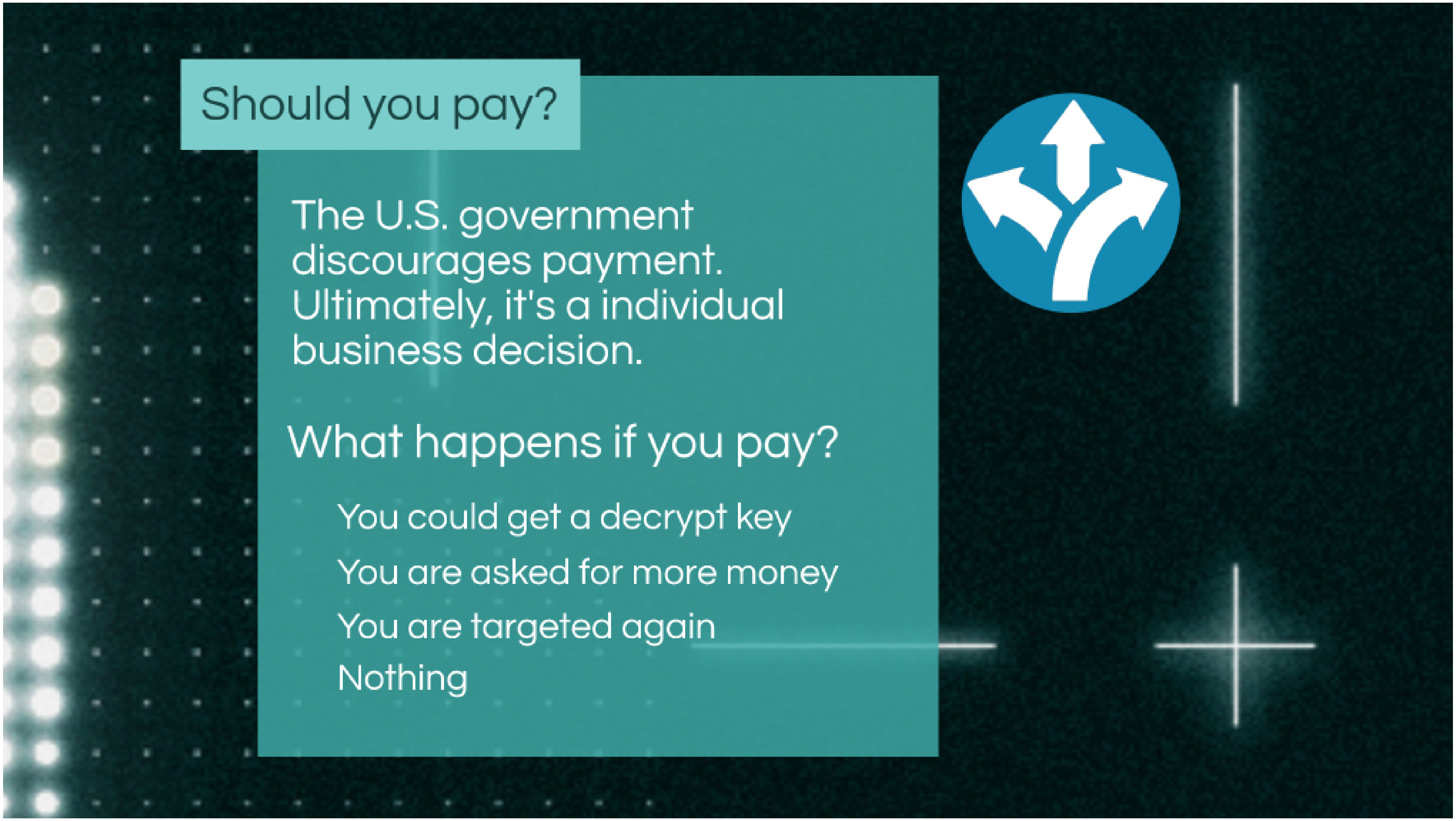


Should you pay?

The U.S. government discourages payment. Ultimately, it's a individual business decision.

What happens if you pay?

- You could get a decrypt key
- You are asked for more money
- You are targeted again



Should you pay?

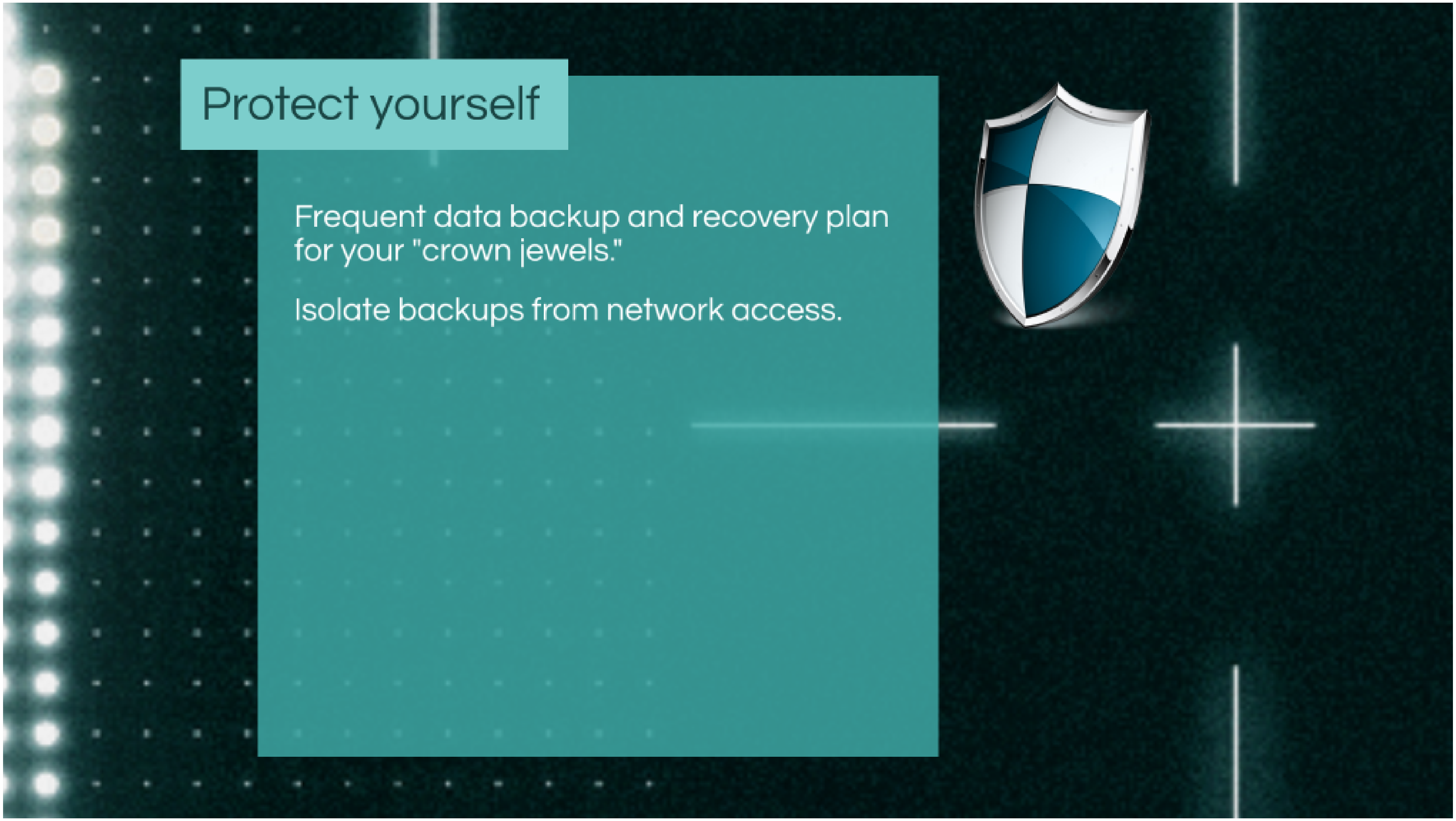
The U.S. government discourages payment. Ultimately, it's a individual business decision.

What happens if you pay?

- You could get a decrypt key
- You are asked for more money
- You are targeted again
- Nothing

Protect yourself

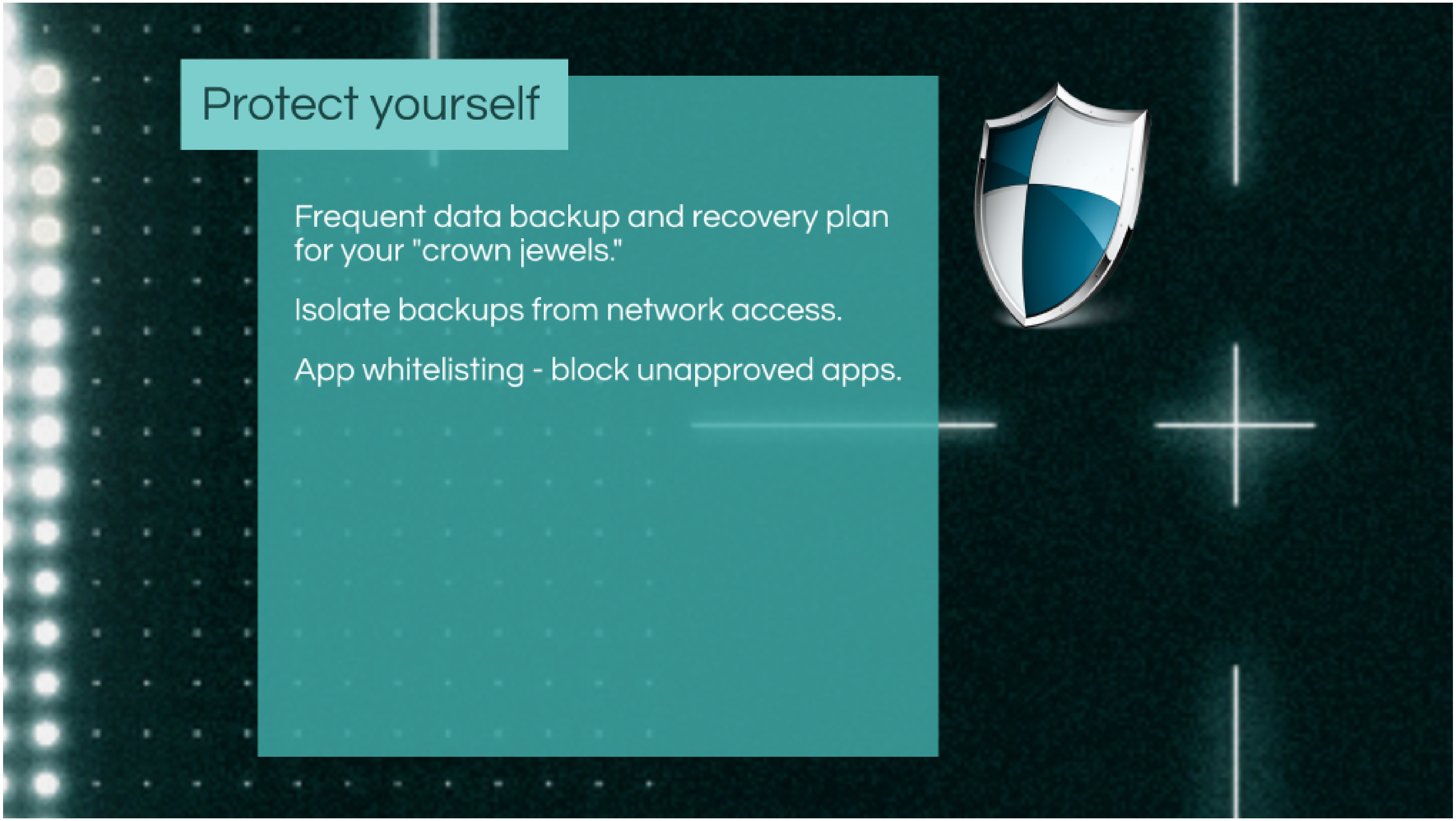
Frequent data backup and recovery plan for your "crown jewels."



Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

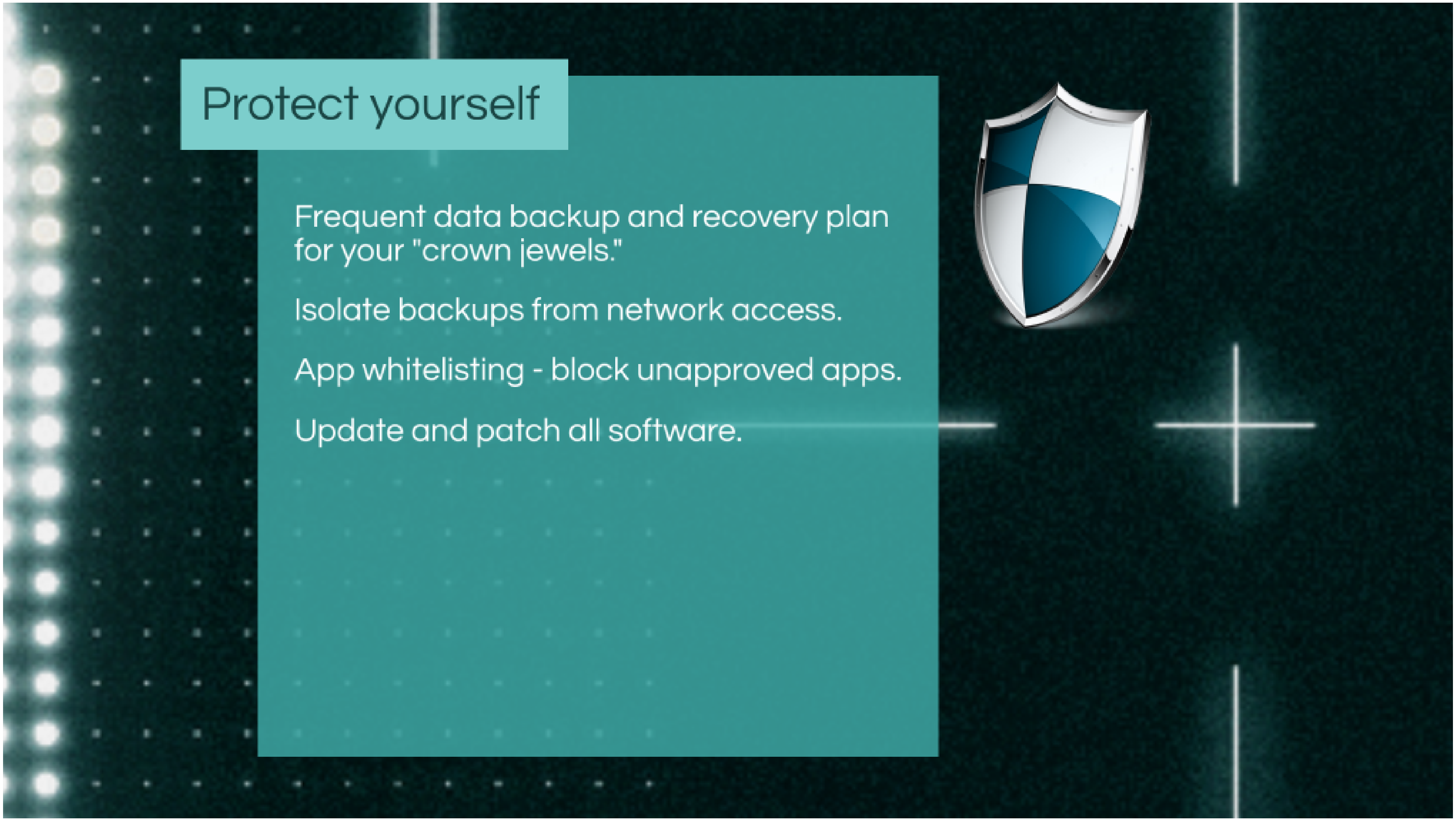


Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

App whitelisting - block unapproved apps.



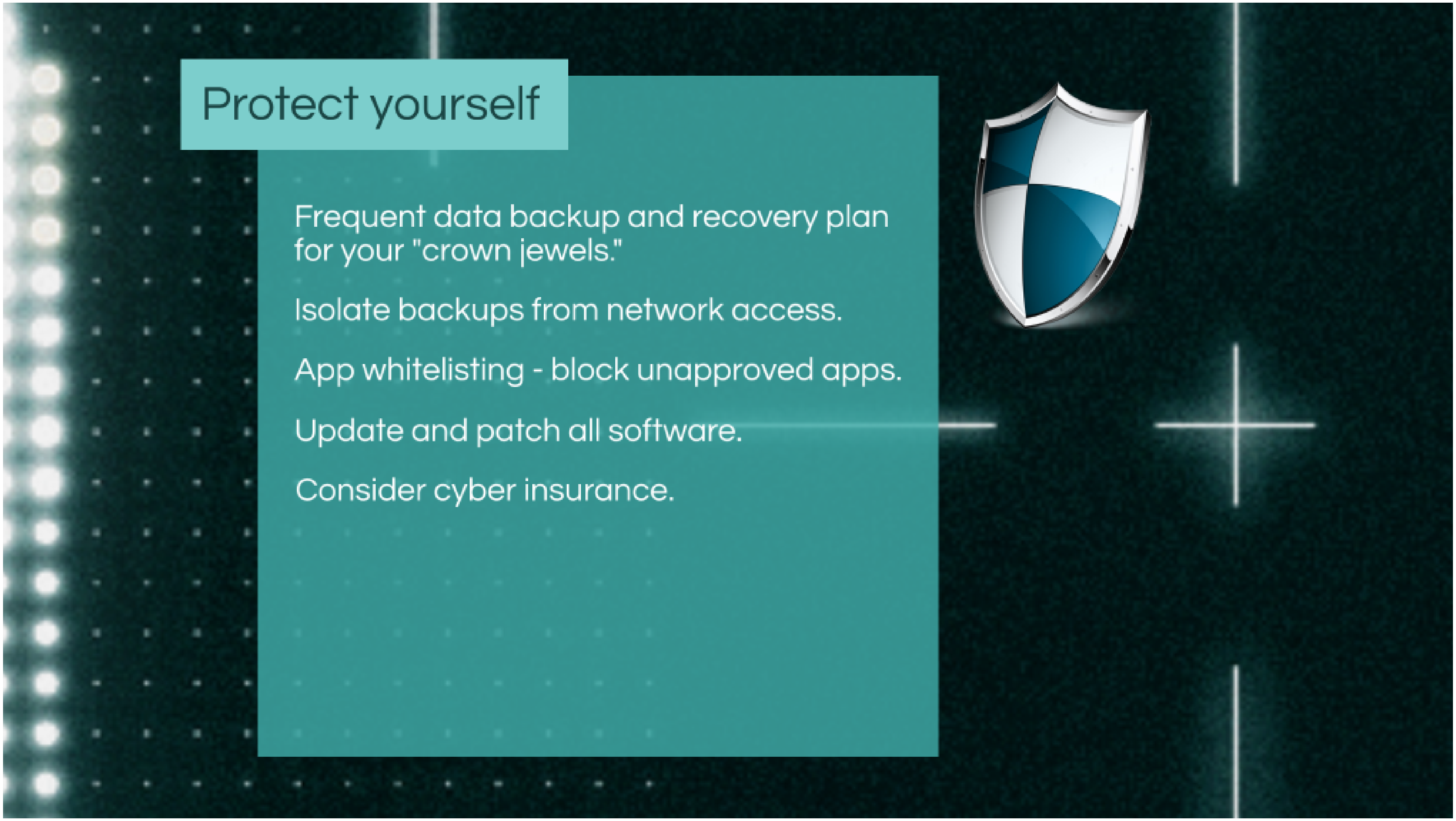
Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

App whitelisting - block unapproved apps.

Update and patch all software.



Protect yourself

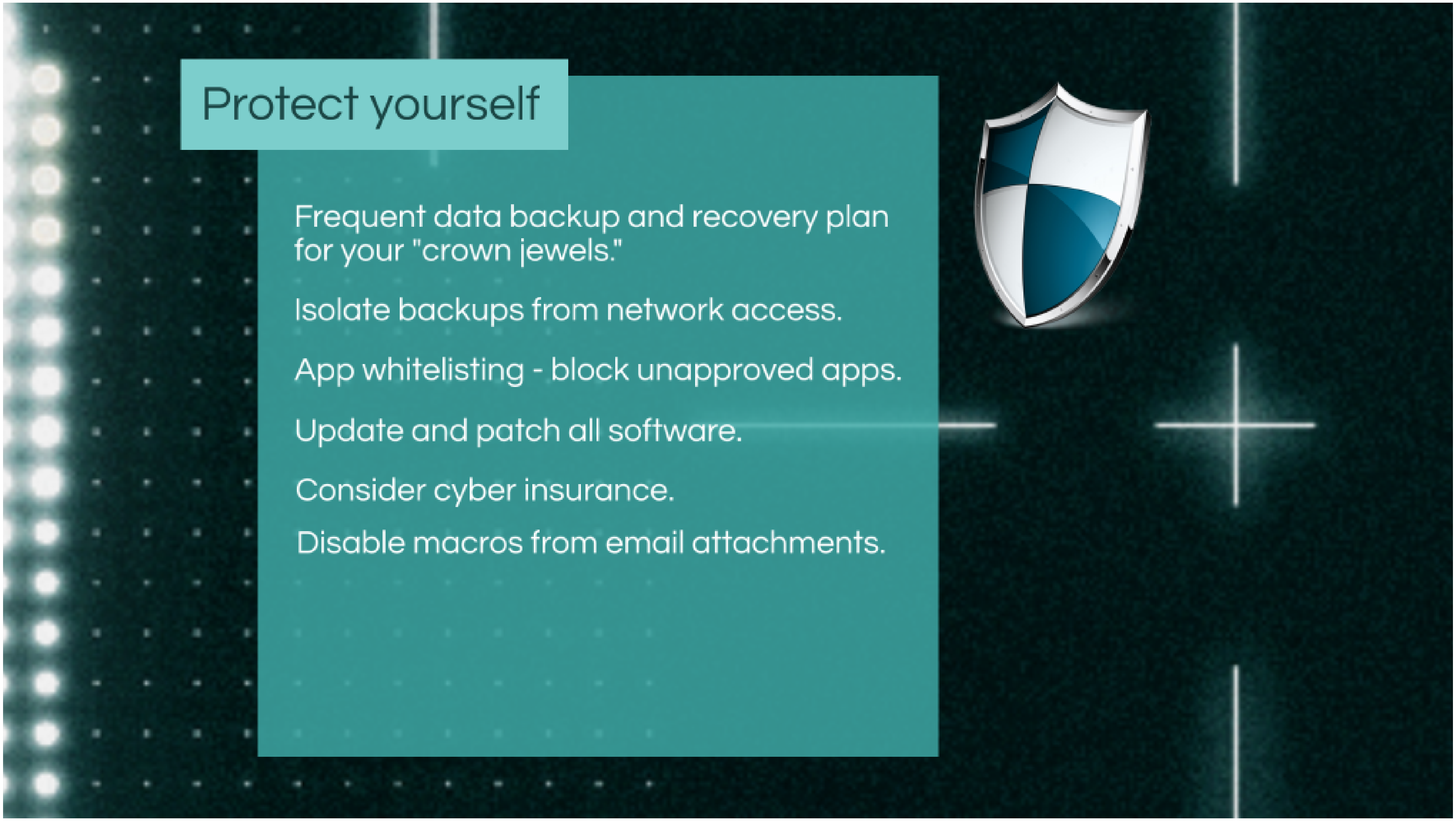
Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

App whitelisting - block unapproved apps.

Update and patch all software.

Consider cyber insurance.



Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

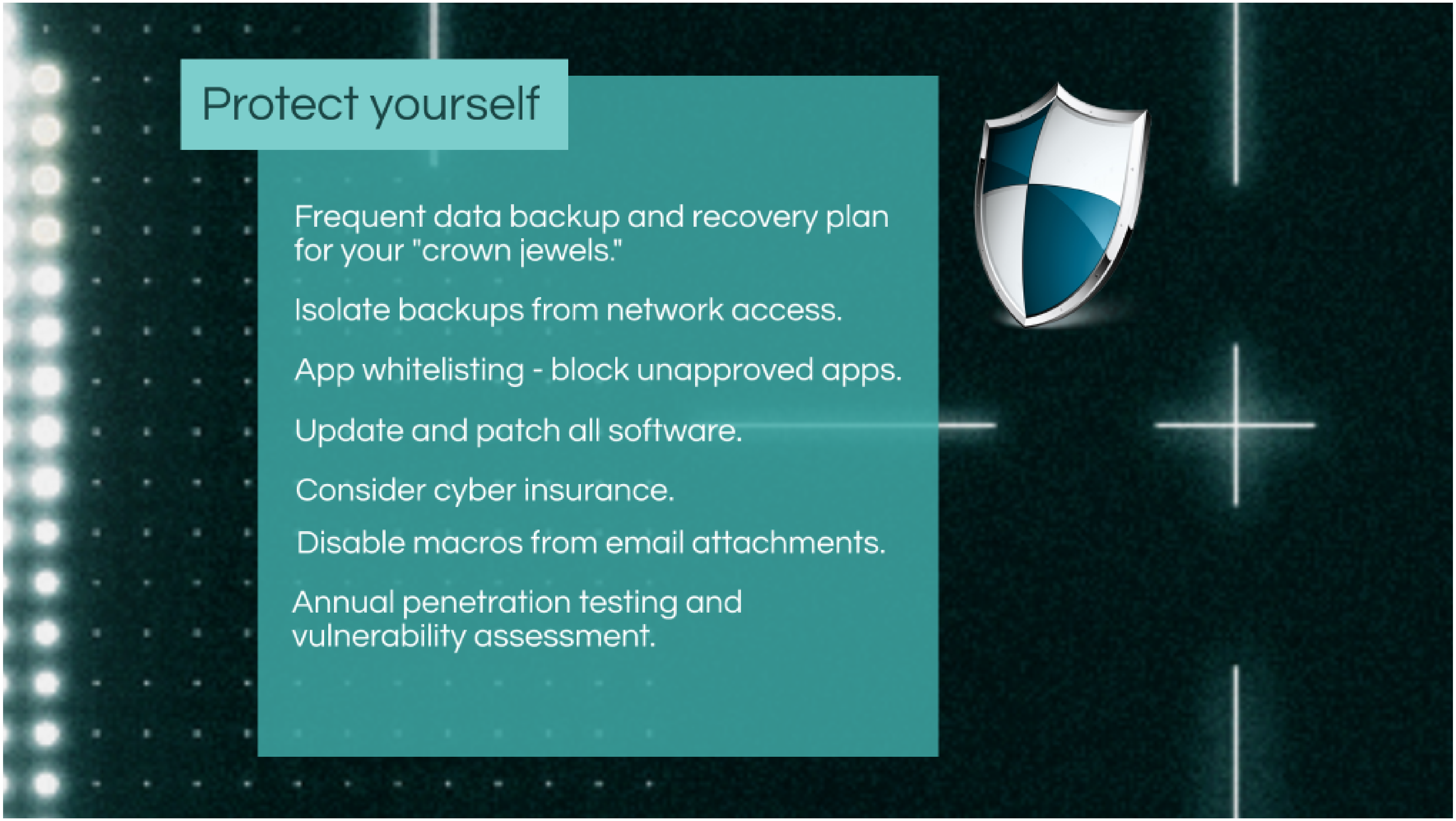
Isolate backups from network access.

App whitelisting - block unapproved apps.

Update and patch all software.

Consider cyber insurance.

Disable macros from email attachments.



Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

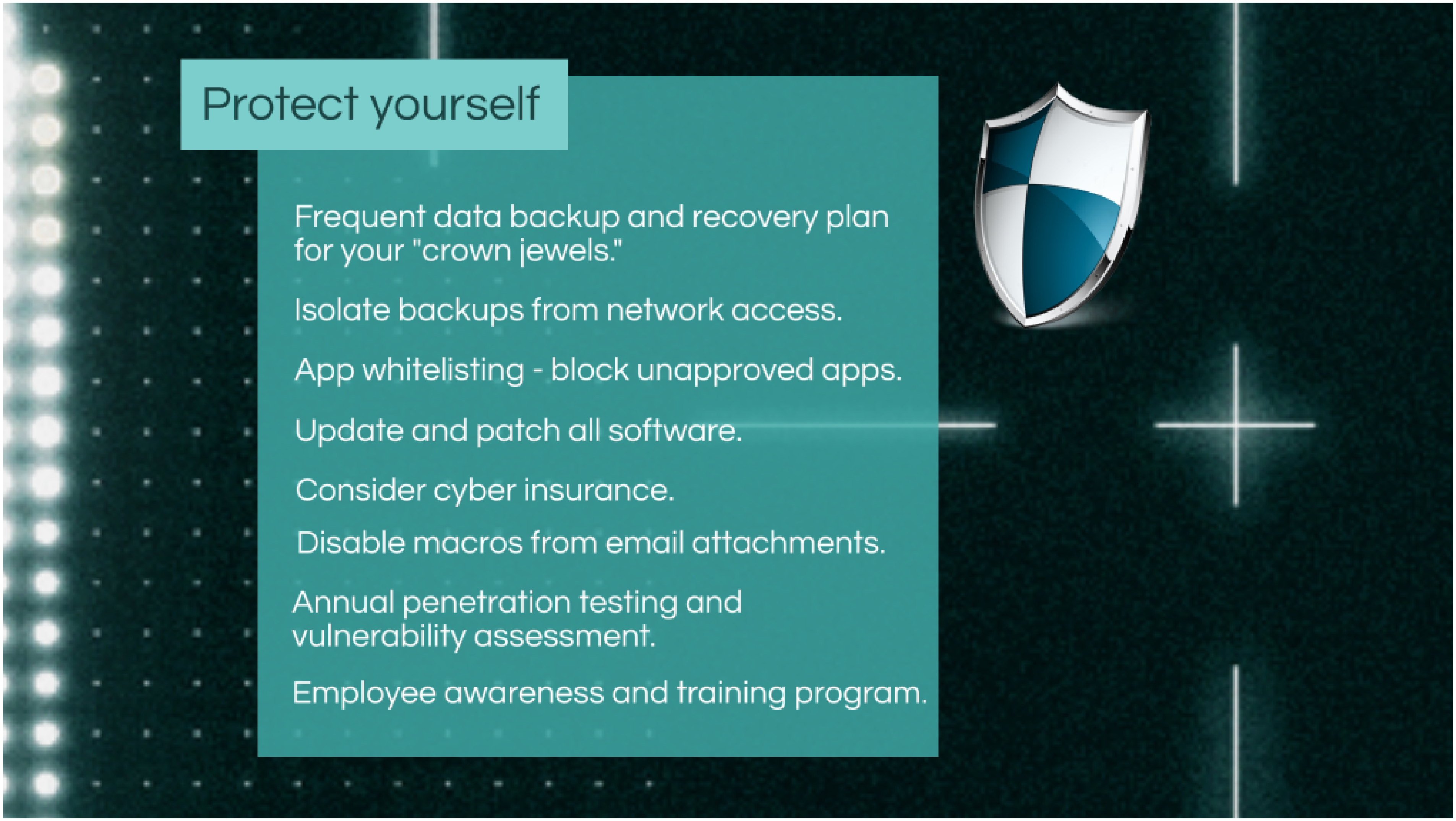
App whitelisting - block unapproved apps.

Update and patch all software.

Consider cyber insurance.

Disable macros from email attachments.

Annual penetration testing and vulnerability assessment.



Protect yourself

Frequent data backup and recovery plan for your "crown jewels."

Isolate backups from network access.

App whitelisting - block unapproved apps.

Update and patch all software.

Consider cyber insurance.

Disable macros from email attachments.

Annual penetration testing and vulnerability assessment.

Employee awareness and training program.

GLOBAL THREATS TO LOCAL BUSINESS: EMAIL COMPROMISE & RANSOMWARE

What is the Threat?

Overview

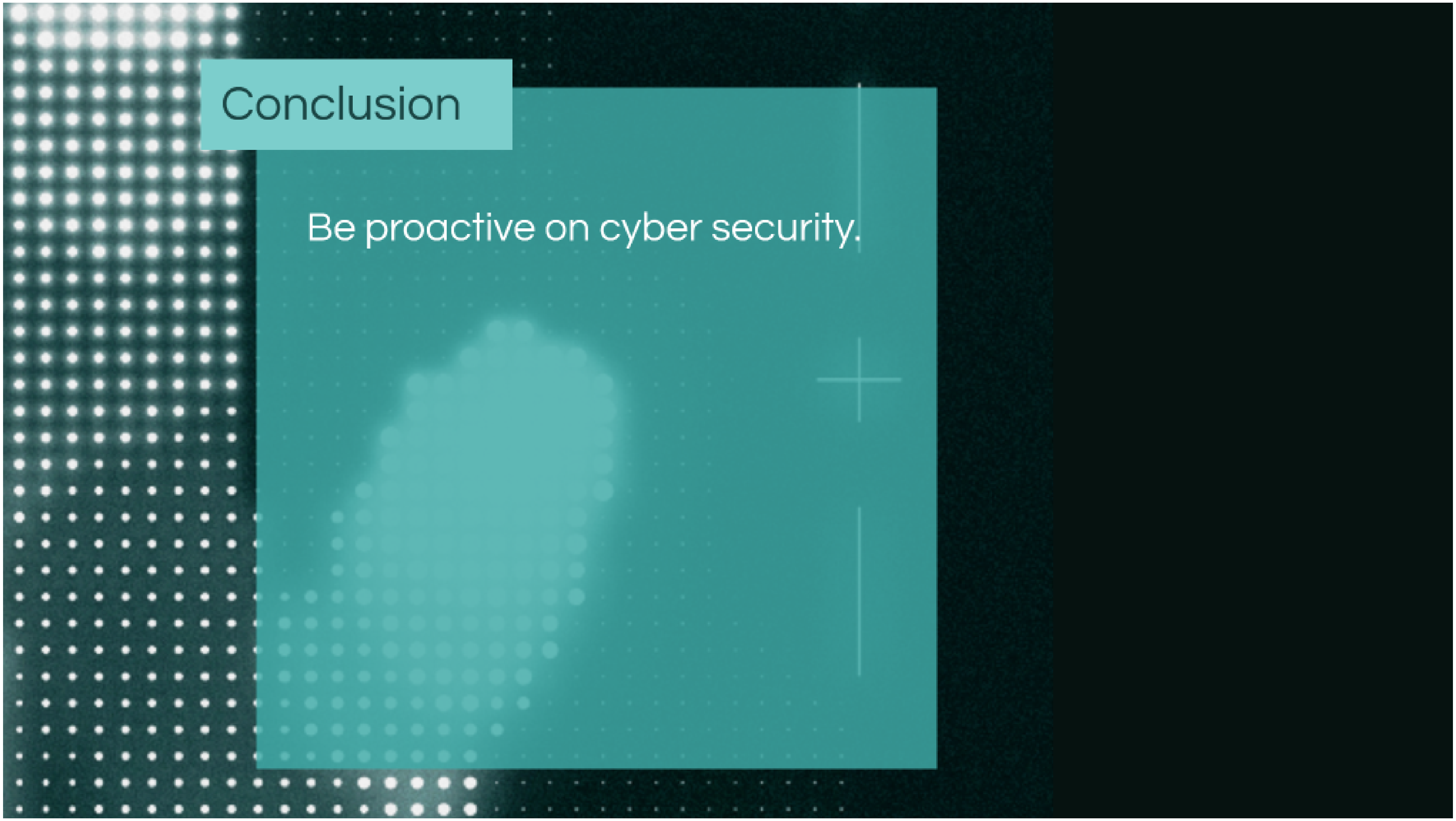
Business Email Compromise

Ransomware

Conclusion

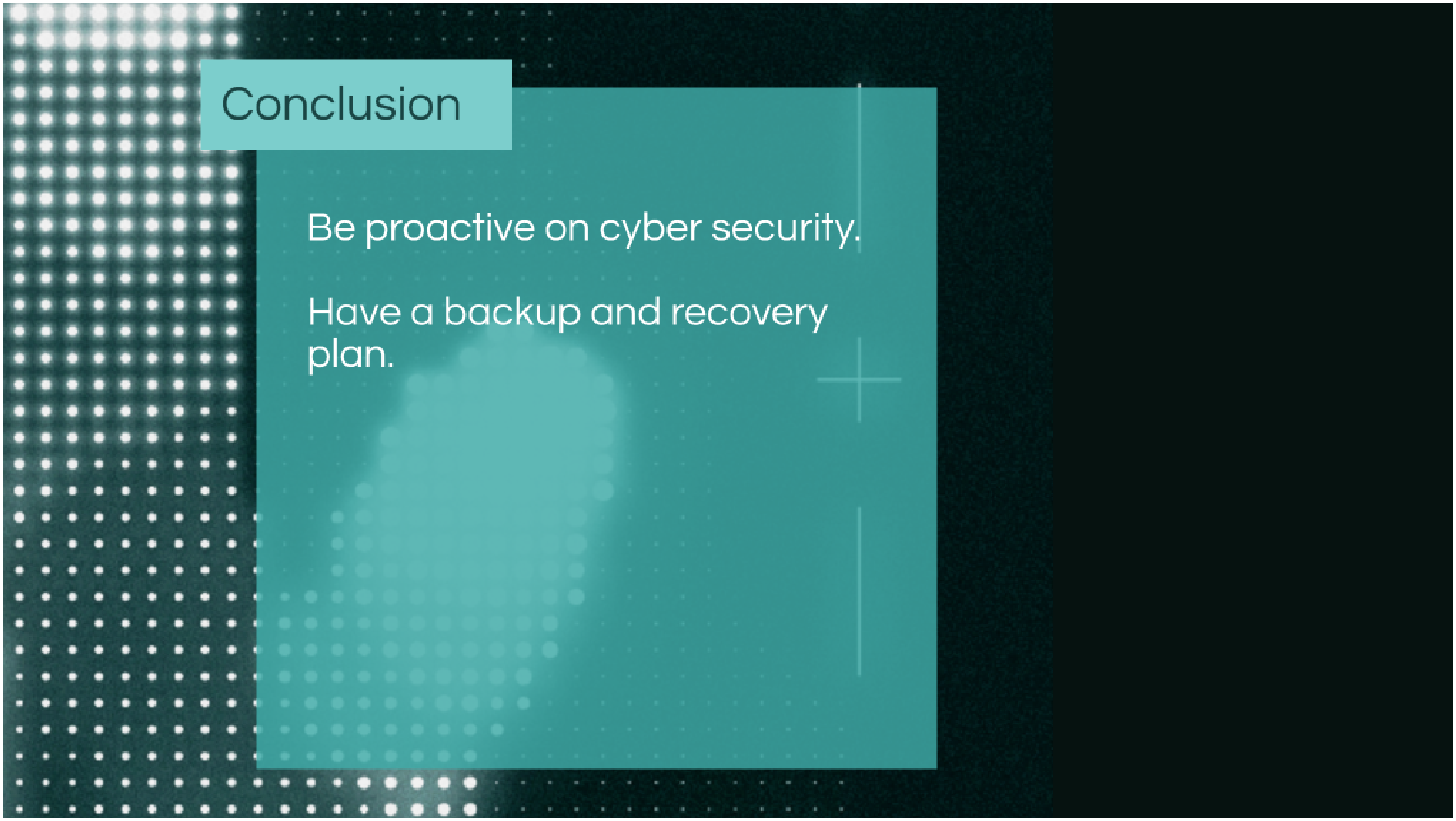
THE END

A public service by
The San Mateo County
District Attorney's Office



Conclusion

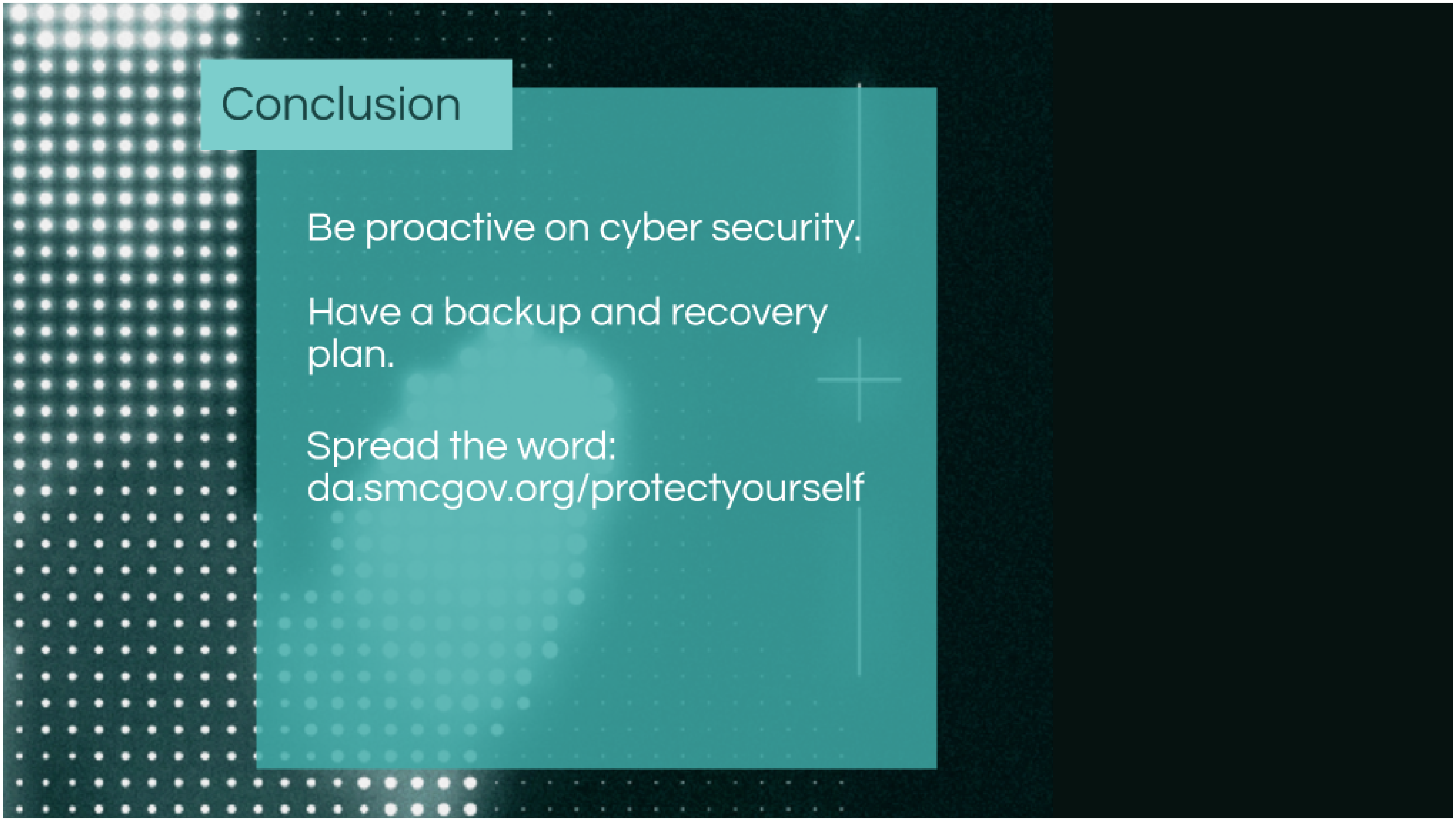
Be proactive on cyber security.



Conclusion

Be proactive on cyber security.

Have a backup and recovery plan.

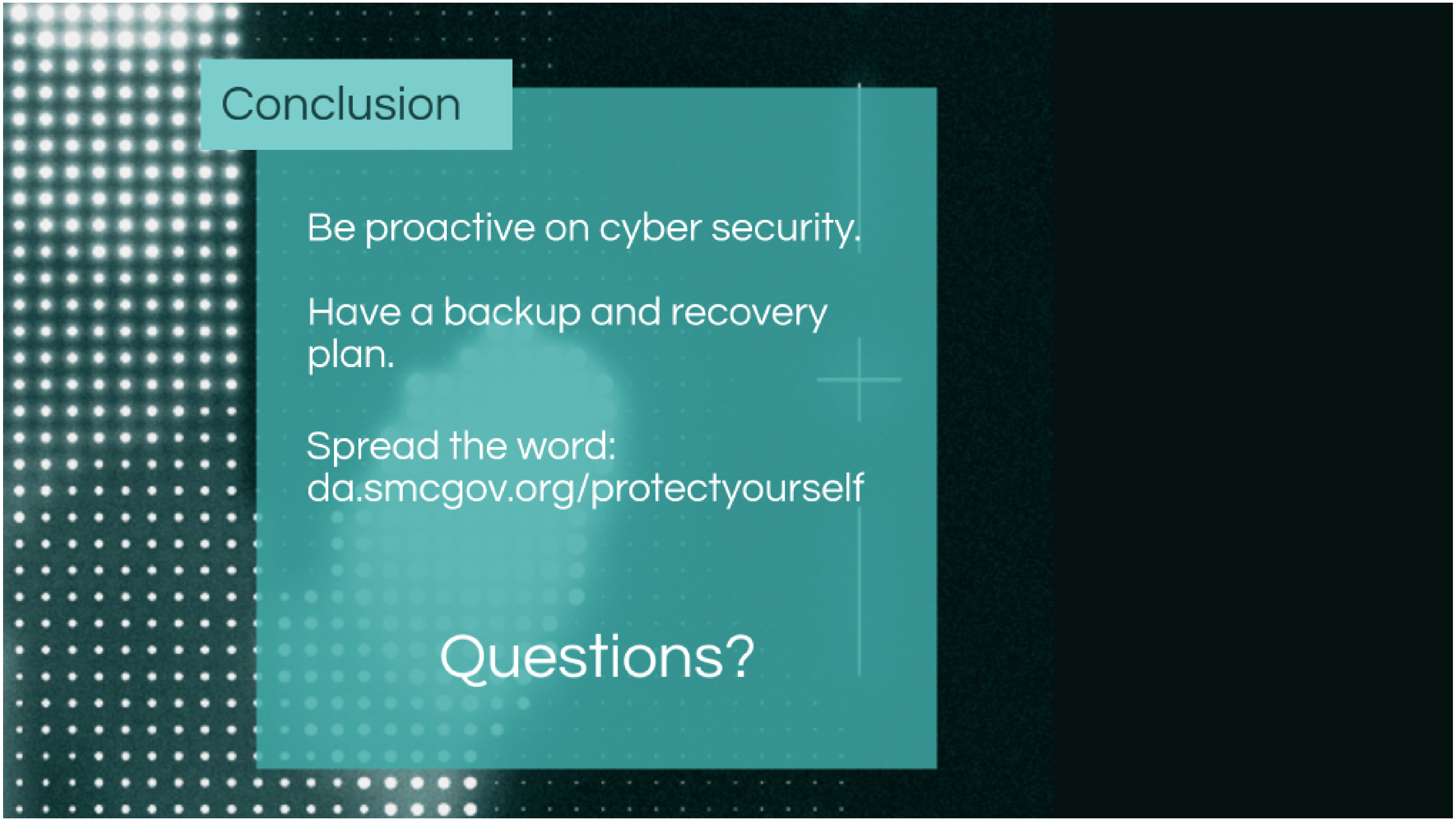


Conclusion

Be proactive on cyber security.

Have a backup and recovery plan.

Spread the word: da.smcgov.org/protectyourself



Conclusion

Be proactive on cyber security.

Have a backup and recovery plan.

Spread the word: da.smcgov.org/protectyourself

Questions?

GLOBAL THREATS TO LOCAL BUSINESS: **EMAIL COMPROMISE & RANSOMWARE**

What is the Threat?

Overview

Business Email Compromise

Ransomware

Conclusion

A public service by
The San Mateo County
District Attorney's Office