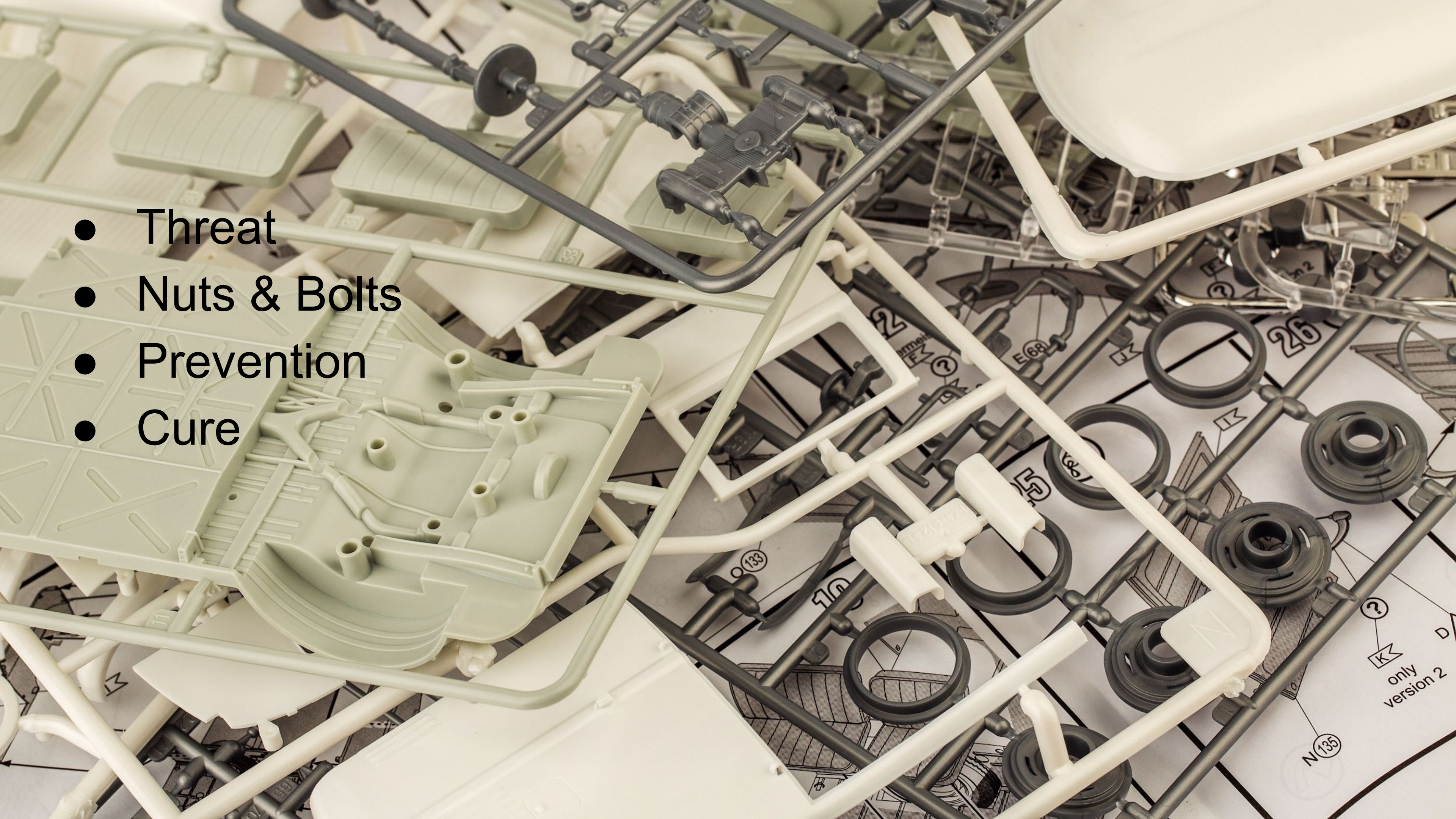
Email Account Compromise

2021: $ 2, 400, 000, 000



- Threat
- Nuts & Bolts
- Prevention
- Cure

The Threat

Who are they?

Individuals

Ad-hoc Networks

Cybercrime Business

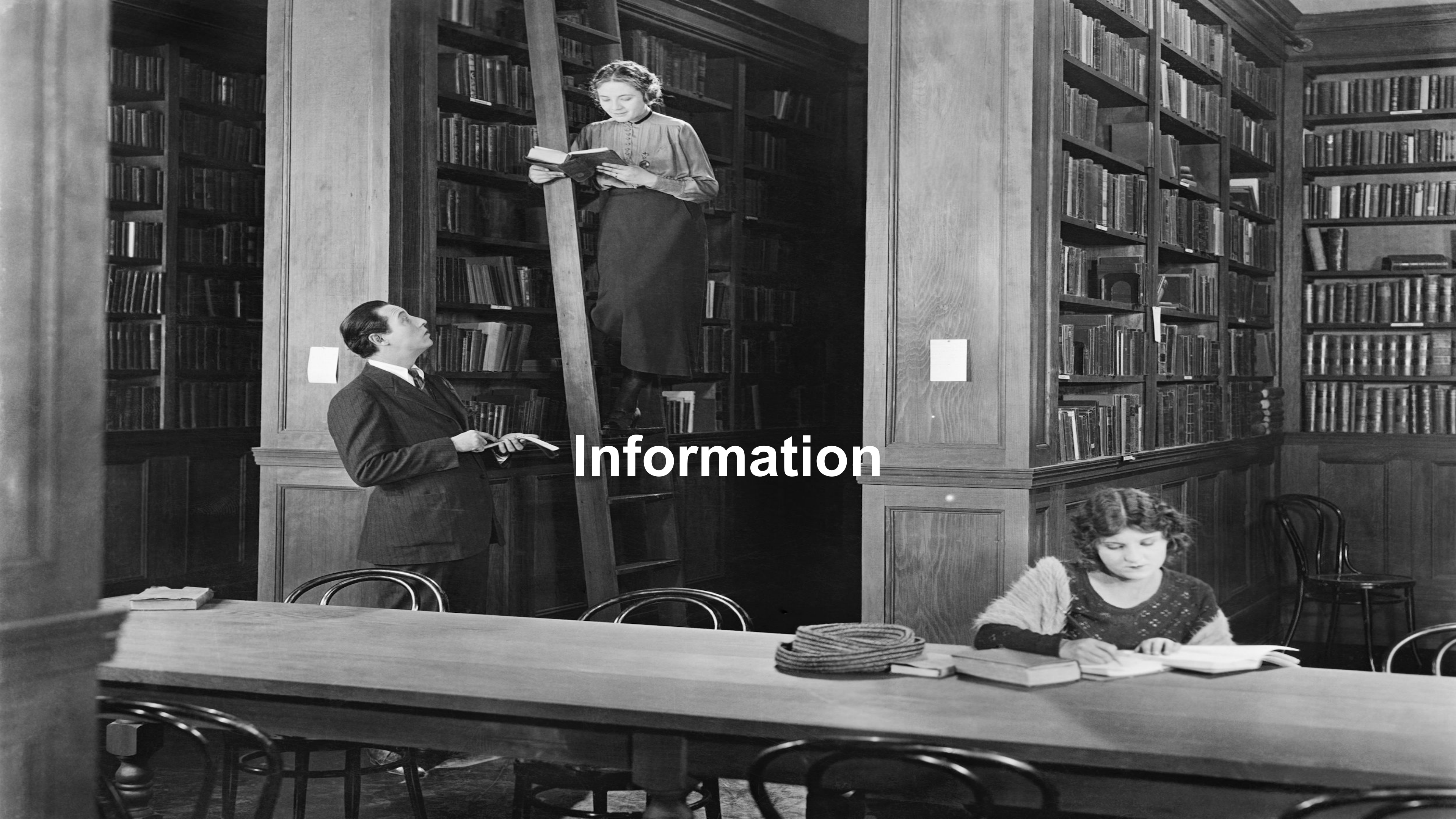
Organised Crime

Countries

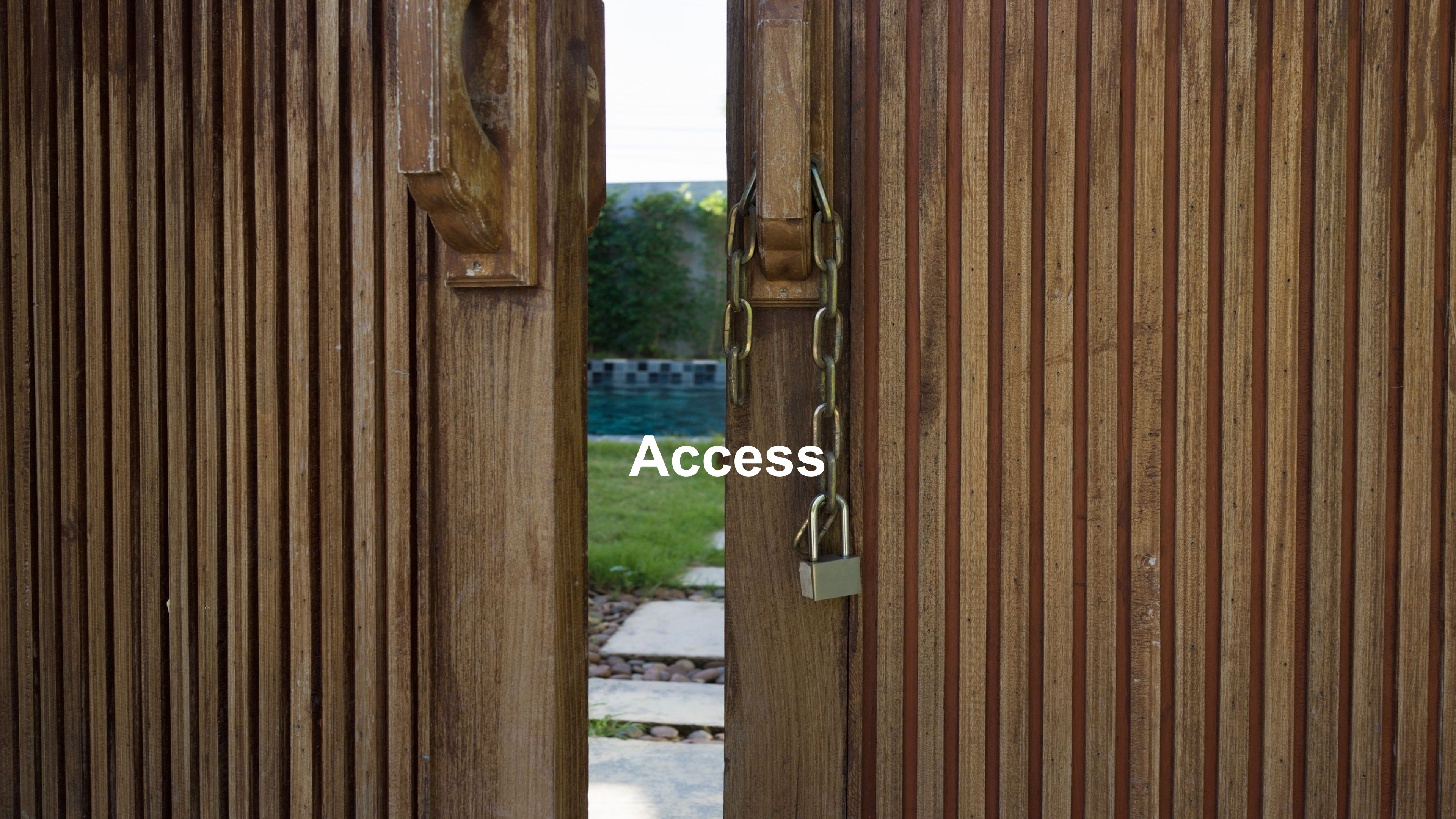
What do they want?

THE UNITED STATES OF AMERICA
KH 49899764 A
HL 43420465 G
ONE HUNDRED DOLLARS
100
Secretary of the Treasury.

Money



Information



Access

Nuts and Bolts

How do they gain access?

Social Engineering

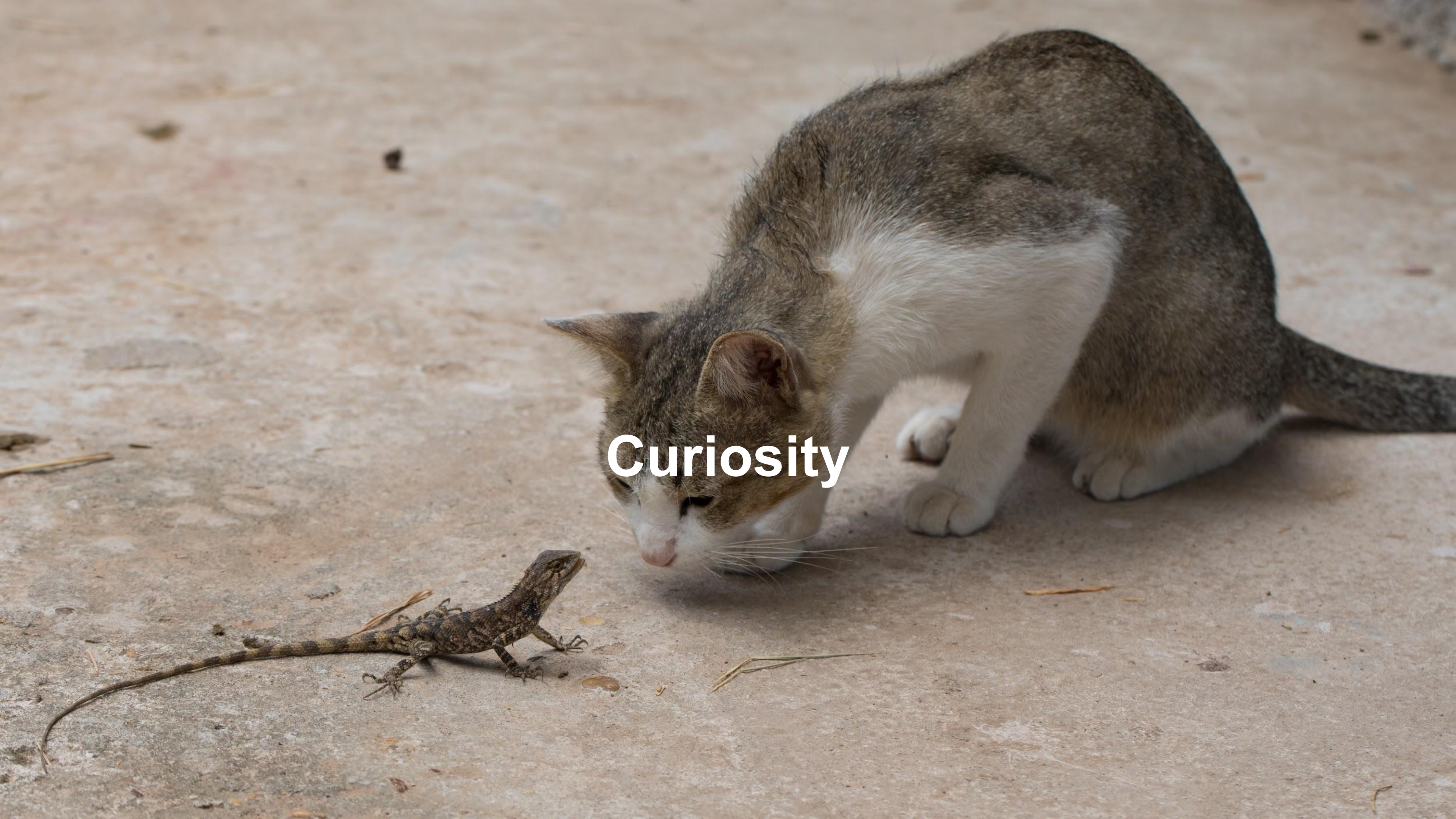
Greed

THE UNITED STATES OF AMERICA
100
KH 49899764 A
ONE HUNDRED DOLLARS
HL 43420465 G
Secretary of the Treasury

$ave Right NOW!
$ave Right EVERYDAY!
SANPELLEGRINO
ARANCIATA
2.29
2.99
ON SALE NOW! SAVE .50
1.59
ON SALE NOW! SAVE .70
$ave Right NOW!
2.59
ON SALE NOW! SAVE .70
1.99
40% OFF SAVE 1.50
3.29
5.19
1.49
5.49
2.99

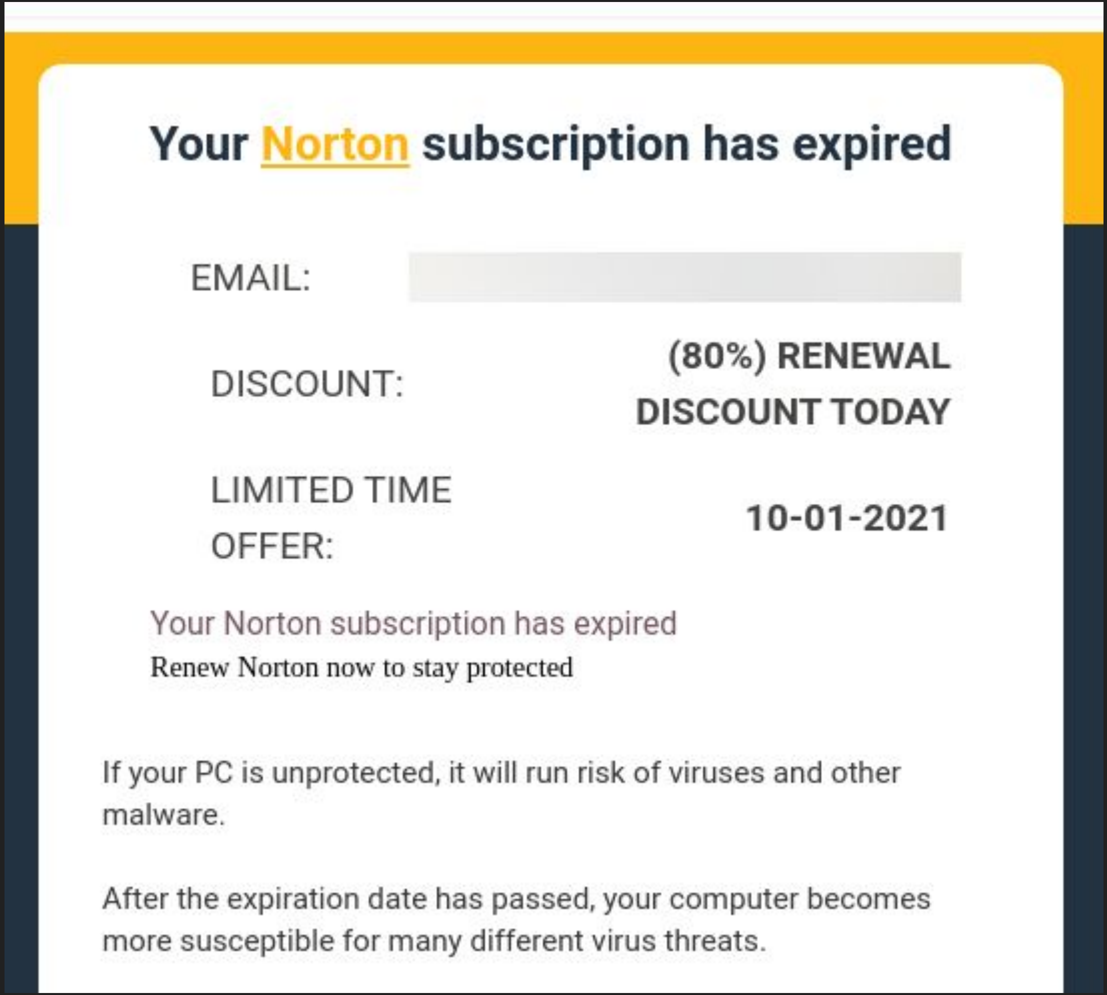
Urgency

Strong Emotions



Curiosity

Examples



Your Norton subscription has expired

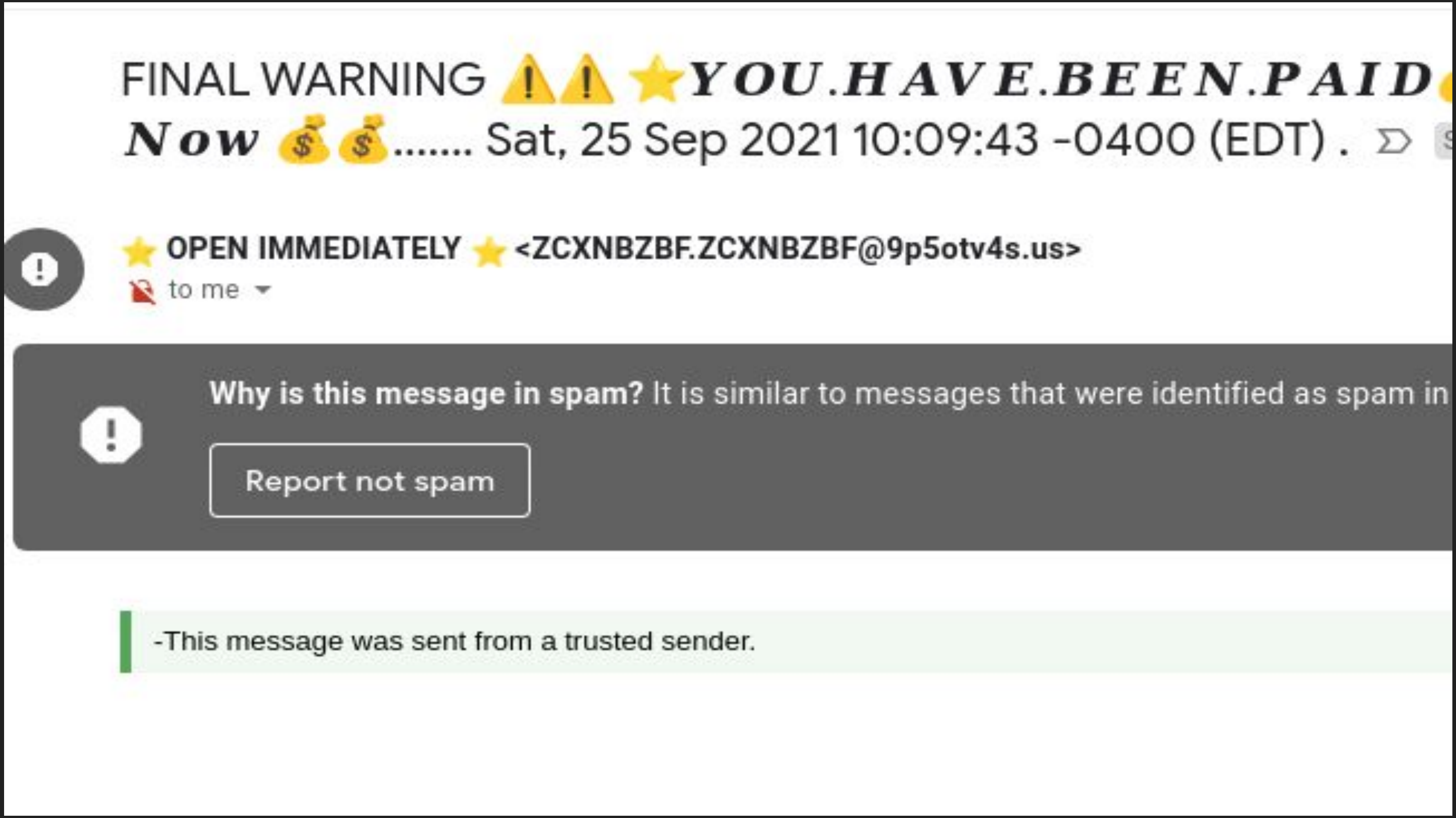
EMAIL:	[redacted]
DISCOUNT:	(80%) RENEWAL DISCOUNT TODAY
LIMITED TIME OFFER:	10-01-2021

Your Norton subscription has expired

Renew Norton now to stay protected

If your PC is unprotected, it will run risk of viruses and other malware.

After the expiration date has passed, your computer becomes more susceptible for many different virus threats.

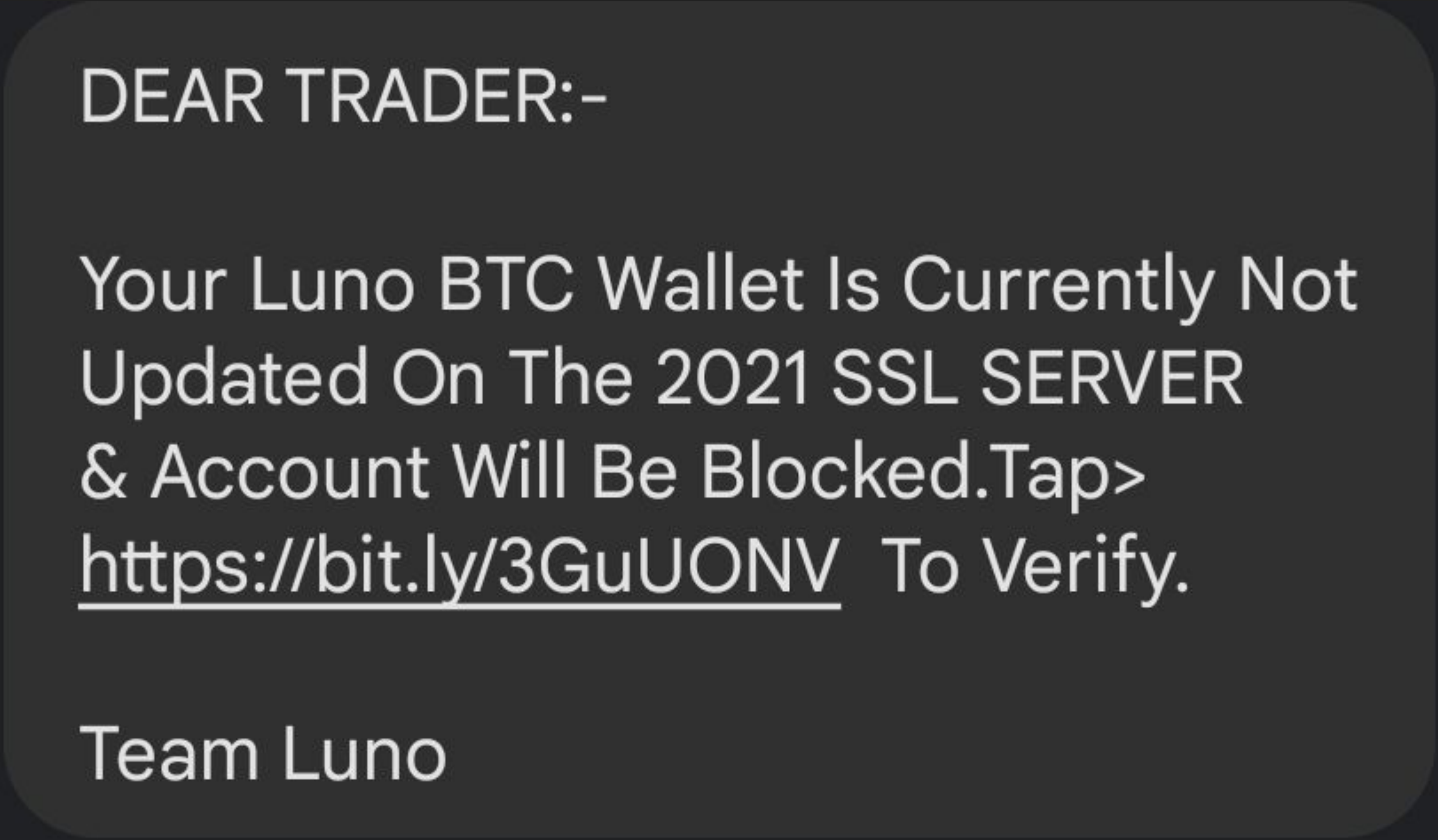


FINAL WARNING ⚠️⚠️ ⭐*YOU.HAVE.BEEN.PAID*
Now 💰💰....... Sat, 25 Sep 2021 10:09:43 -0400 (EDT) .

⭐ **OPEN IMMEDIATELY** ⭐ **<ZCXNBZBF.ZCXNBZBF@9p5otv4s.us>**
to me

Why is this message in spam? It is similar to messages that were identified as spam in

-This message was sent from a trusted sender.



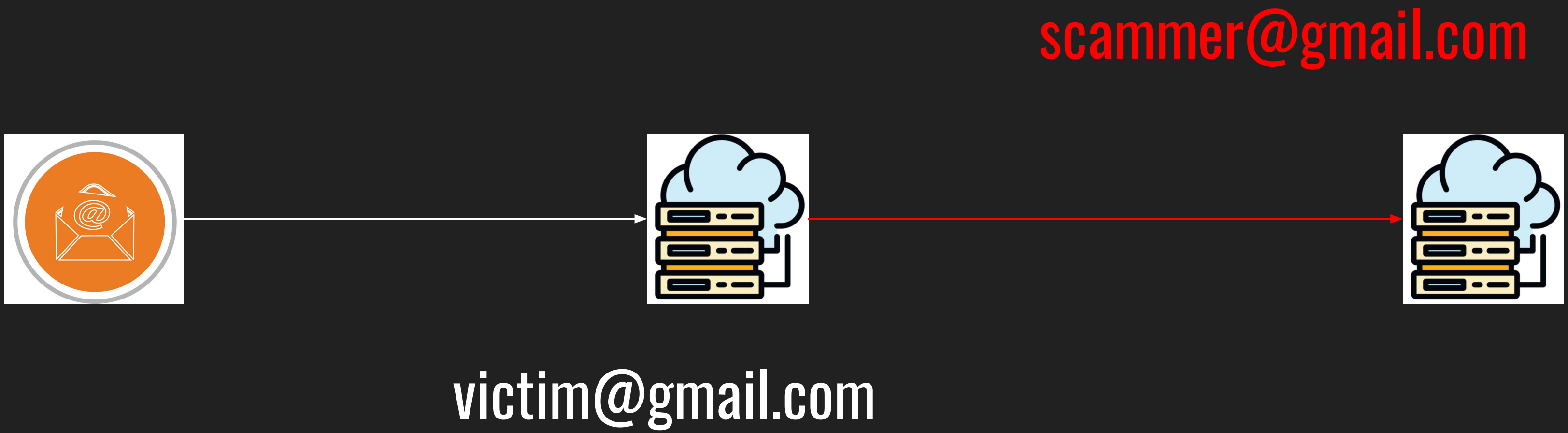
DEAR TRADER:-

Your Luno BTC Wallet Is Currently Not Updated On The 2021 SSL SERVER & Account Will Be Blocked.Tap> https://bit.ly/3GuUONV To Verify.

Team Luno

Exploiting the access

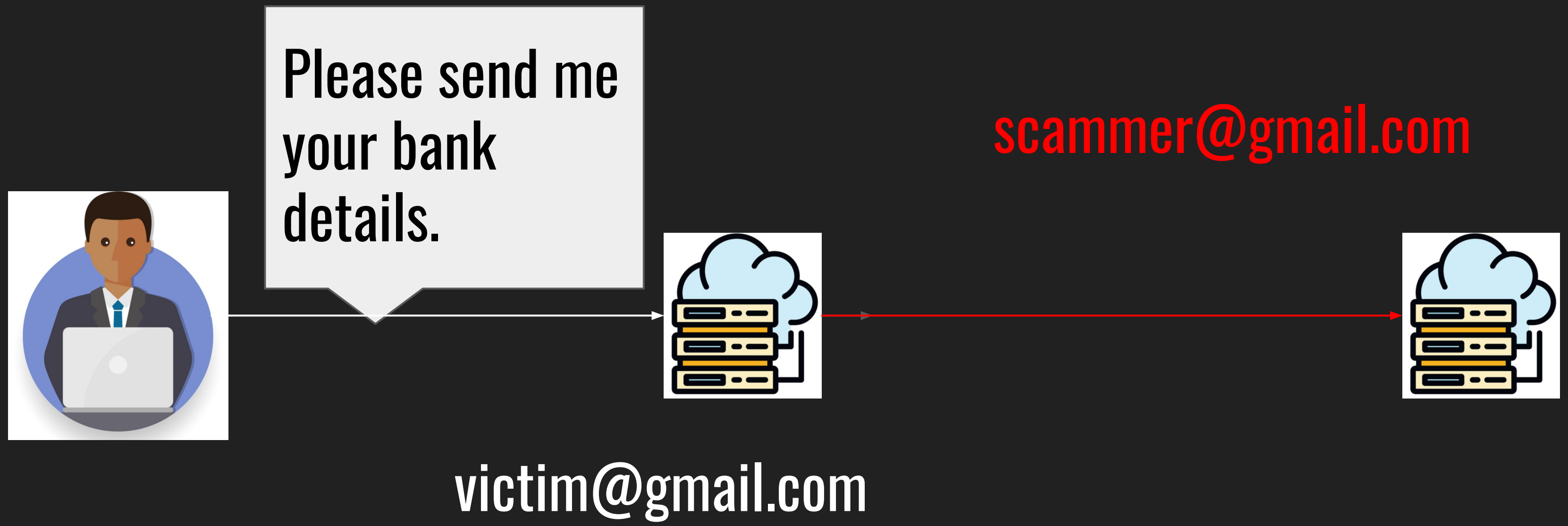
Step 1: Forward victim's emails



scammer@gmail.com

victim@gmail.com

Step 2: Wait for a suitable email

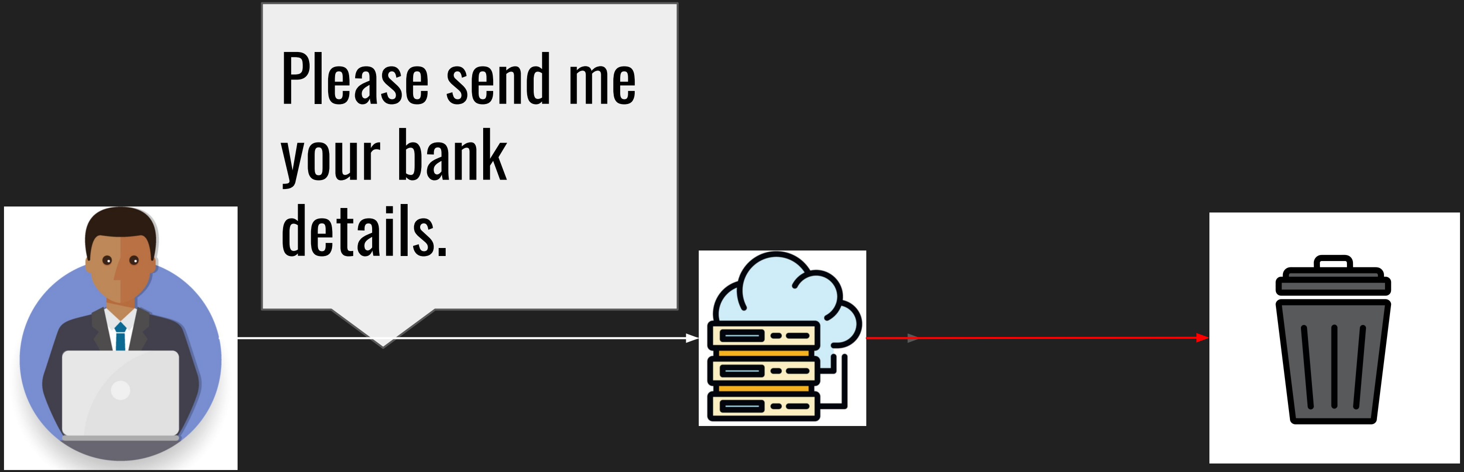


Please send me your bank details.

scammer@gmail.com

victim@gmail.com

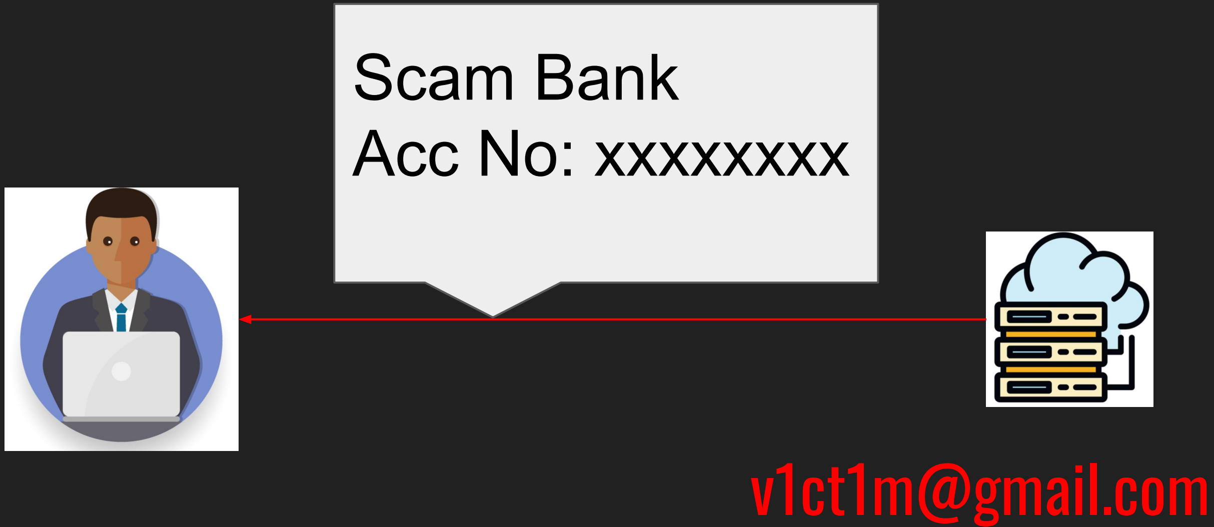
Step 3: Remove the evidence



Please send me your bank details.

victim@gmail.com

Step 4: Control the transaction



Scam Bank
Acc No: xxxxxxxx

v1ct1m@gmail.com

Prevention

Don’t trust your mailbox

- Watch for things that seem ‘off’:
  - sender address
  - time
  - content
- Don’t click on links
- Confirm payment details out of band

Protect Yourself

- Use strong, unique passwords
- Implement two-factor authentication
- Check your email settings regularly
- Apply updates to your devices ASAP
- Training
- Remove the stigma

Protect others

- Send business email from a custom domain rather than a generic mailbox (e.g. @gmail.com, @outlook.com)
- Give customers channels to validate bank details
- Educate your customers

Cure

Damage Reduction

- Contact your bank
- Contact the police
- Change your email credentials
- Check your settings
- Scan your devices with antivirus software

Secure your environment

- Change other passwords
- Implement MFA
- Preserve data
  - Emails
  - Email logs (from your service provider)

Damage Assessment

- Are there perhaps other incidents that have yet to come to light?
- Are there other mailboxes that may have been compromised.

Thank you!

https://www.capefox.co/staying-safe-online

info@capefox.co

Sources

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Images

All images from Shutterstock, except:

https://commons.wikimedia.org/wiki/File:Curious_cat_starring_at_a_lizard.jpg

https://commons.wikimedia.org/wiki/File:Empty_supermarket_shelves_before_Hurricane_Sandy,_Montgomery,_NY.jpg

https://commons.wikimedia.org/wiki/File:Rage.jpg