

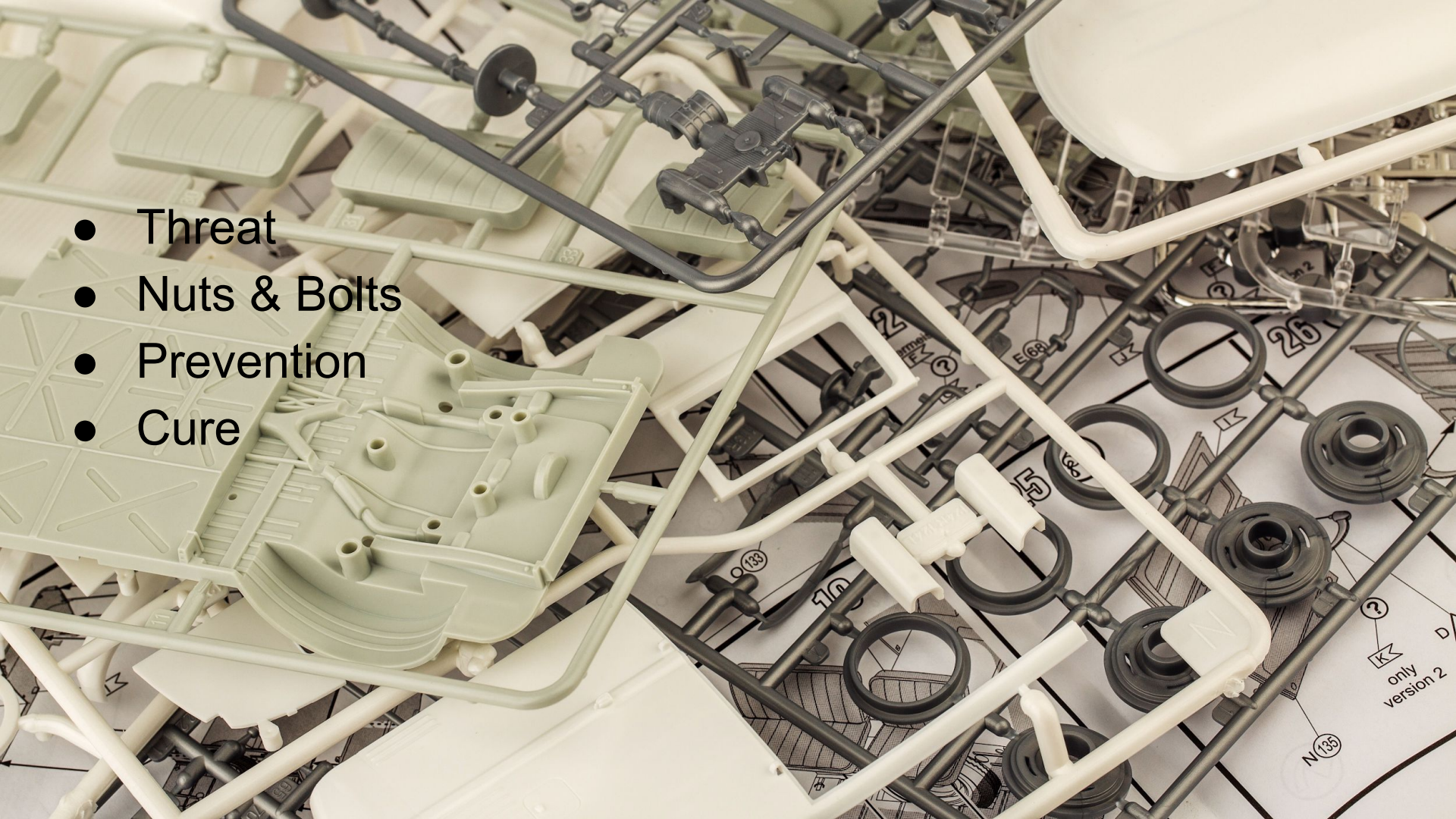
A blue-tinted photograph of a metal padlock on a chain-link fence. The padlock is silver and has a textured, rectangular body. It is attached to a chain-link fence that is also blue-tinted. The background is blurred, showing more of the fence and some indistinct shapes. The text "Email Account Compromise" is overlaid in red on the center of the image.

# Email Account Compromise

2021: \$ 2, 400, 000, 000



- Threat
- Nuts & Bolts
- Prevention
- Cure



# The Threat

Who are they?



**Individuals**



**Ad-hoc Networks**

A person wearing a white face mask is holding a circular wooden sign with both hands. The sign has the word 'OPEN' in large, bold, black letters. Below 'OPEN' is the word 'Welcome' in a smaller, black, sans-serif font. The sign is suspended by a piece of twine. The background is a blurred interior of a cafe or shop with warm lighting and shelves.

**OPEN**

**Cybercrime Business**

*Welcome*



A group of six men standing in a parking garage. They are dressed in dark, tactical-style clothing. The man on the far left holds a white briefcase. The man in the center holds a handgun. The man on the far right also holds a handgun. A dark SUV is parked behind them. The text "Organised Crime" is overlaid in the center.

# Organised Crime

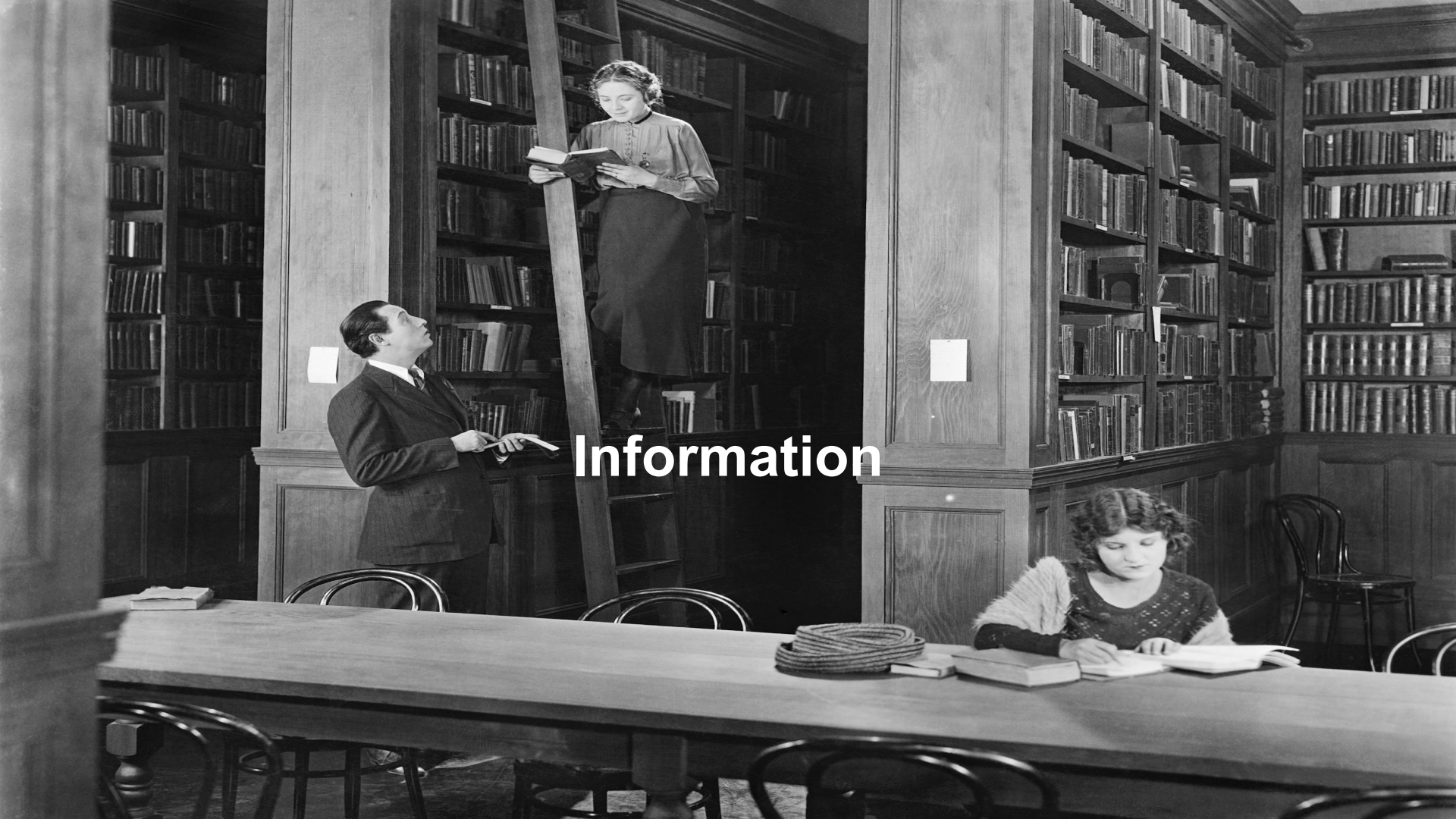


**Countries**

What do they want?



Money



# Information

A close-up photograph of a wooden door made of vertical slats. The door is partially open, revealing a garden path with stone slabs and a blue swimming pool in the background. A metal chain and padlock are attached to the door's handle mechanism. The word "Access" is overlaid in white text on the path.

**Access**

# Nuts and Bolts

How do they gain access?



An aerial, high-angle photograph of a large crowd of people walking on a checkered floor. The floor is composed of large, light-colored square tiles arranged in a grid pattern. The people are seen from above, their shadows cast on the floor. The crowd is dense and moving in various directions. In the center of the image, the words "Social Engineering" are overlaid in a bold, sans-serif font. "Social" is in black, and "Engineering" is in red. The overall scene suggests a busy public space, possibly a transit station or a large indoor arena.

**Social Engineering**



Greed





**Strong Emotions**

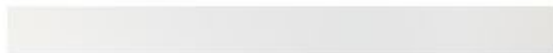
A photograph of a gray and white tabby cat sitting on a light-colored concrete floor. The cat is leaning forward, looking intently at a small, brown lizard that is positioned just in front of its nose. The scene is captured in a close-up, low-angle shot, emphasizing the cat's curiosity. The word "Curiosity" is overlaid in white text on the cat's face.

**Curiosity**

# Examples

## Your Norton subscription has expired

EMAIL:



DISCOUNT:

**(80%) RENEWAL  
DISCOUNT TODAY**

LIMITED TIME

**10-01-2021**

OFFER:

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

Report not spam

-This message was sent from a trusted sender.



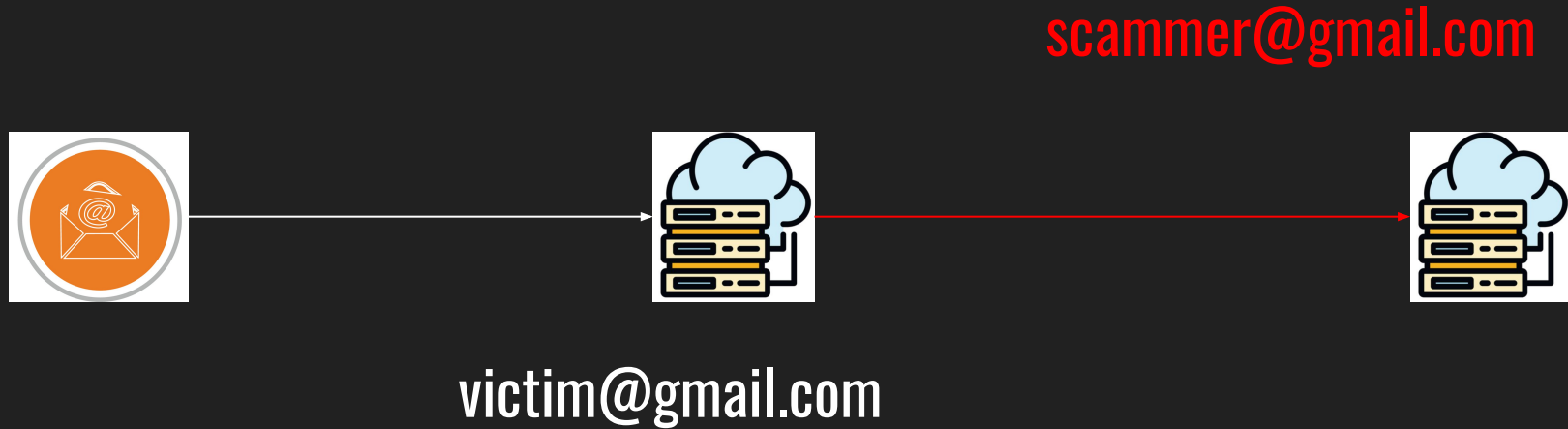
DEAR TRADER:-

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

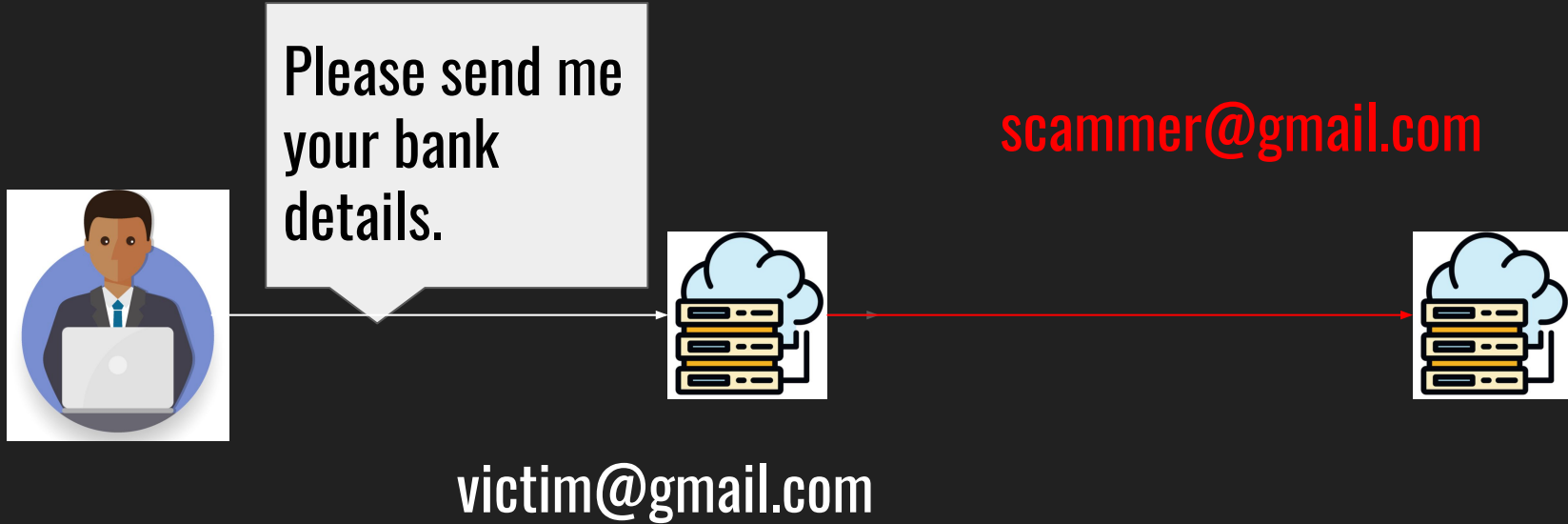
Team Luno

**Exploiting the access**

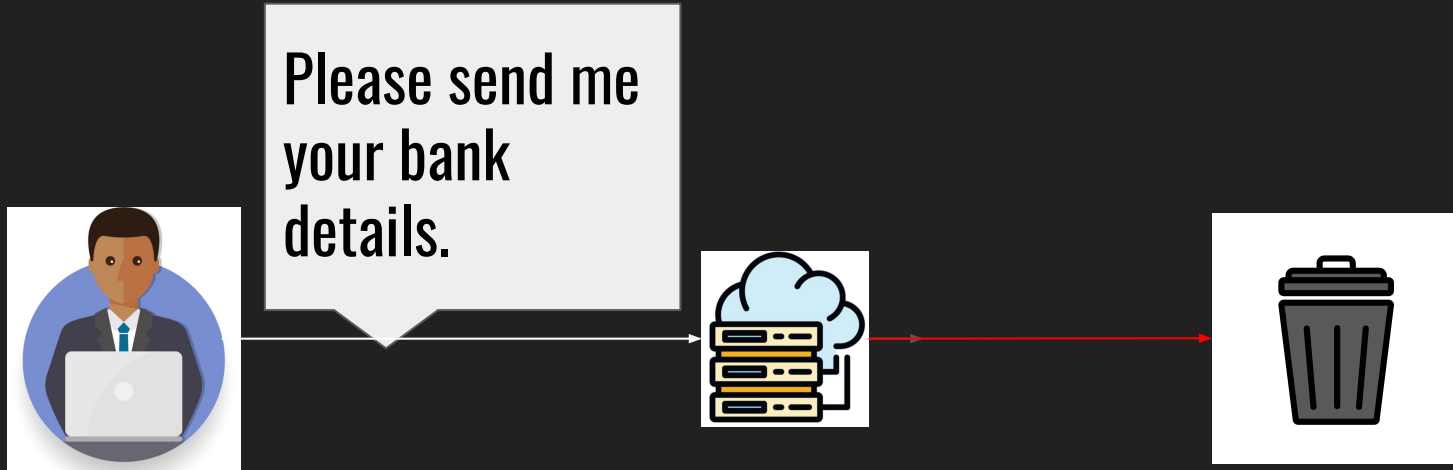
# Step 1: Forward victim's emails



## Step 2: Wait for a suitable email

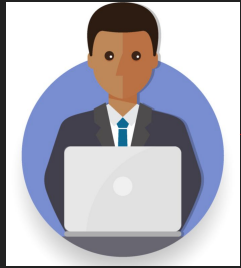


## Step 3: Remove the evidence

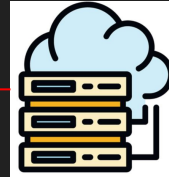


victim@gmail.com

## Step 4: Control the transaction



Scam Bank  
Acc No: xxxxxxxx



[v1ct1m@gmail.com](mailto: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](mailto:info@capefox.co)**

# Sources

[https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](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: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:Empty_supermarket_shelves_before_Hurricane_Sandy,_Montgomery,_NY.jpg)

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