GTMARITIME

data · optimised · secured · delivered

Why do smart people still get Phished?

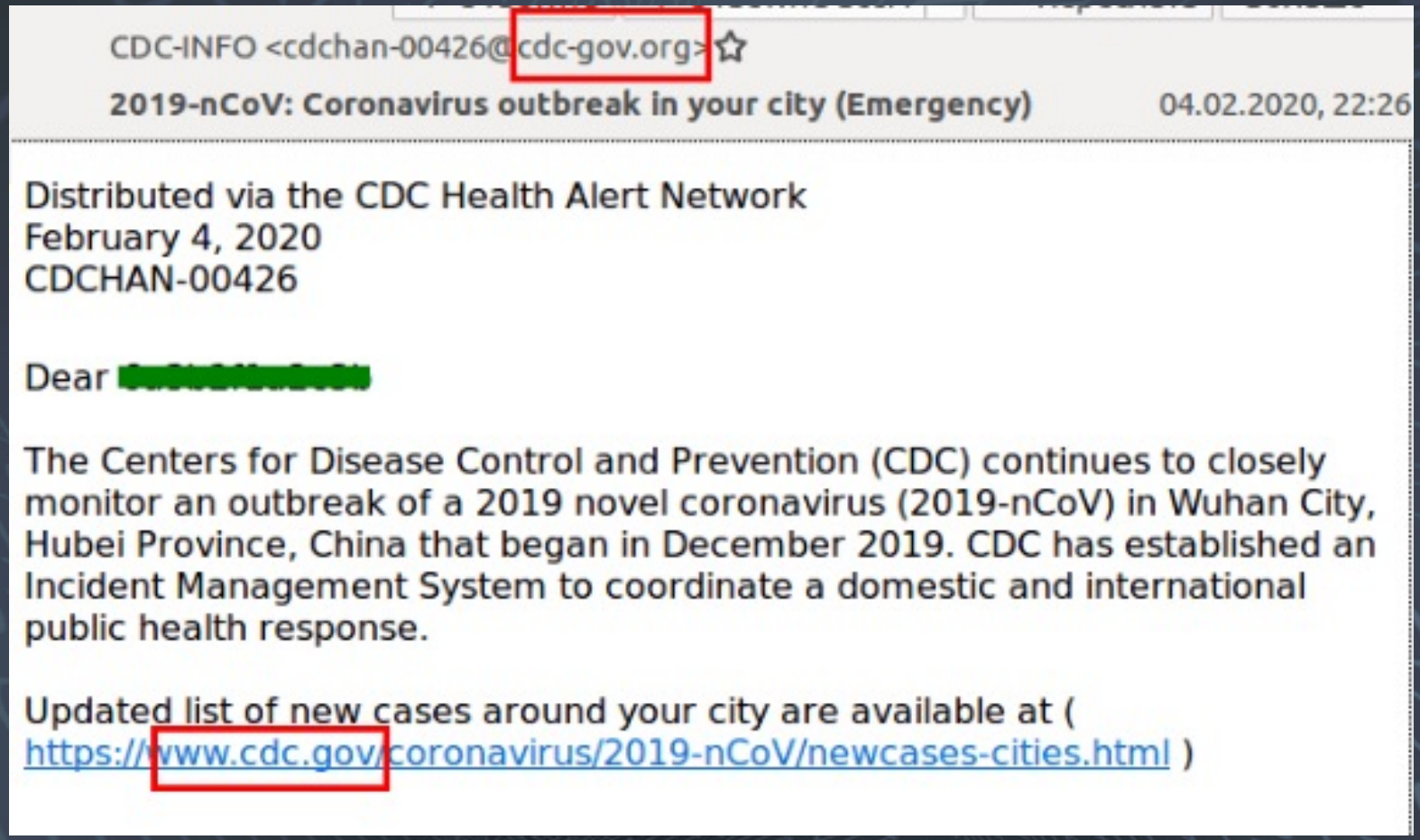
How did that happen to me!

GTMARITIME
data · optimised · secured · delivered

In the early days Phishing attacks were easier to identify.

Often including outlandish claims and with errors in grammar and spelling warning us of the threat.

But today's Phishing attacks present plausible requests appearing from known senders.



CDC-INFO <cdchan-00426@cdc-gov.org>

2019-nCoV: Coronavirus outbreak in your city (Emergency) 04.02.2020, 22:26

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

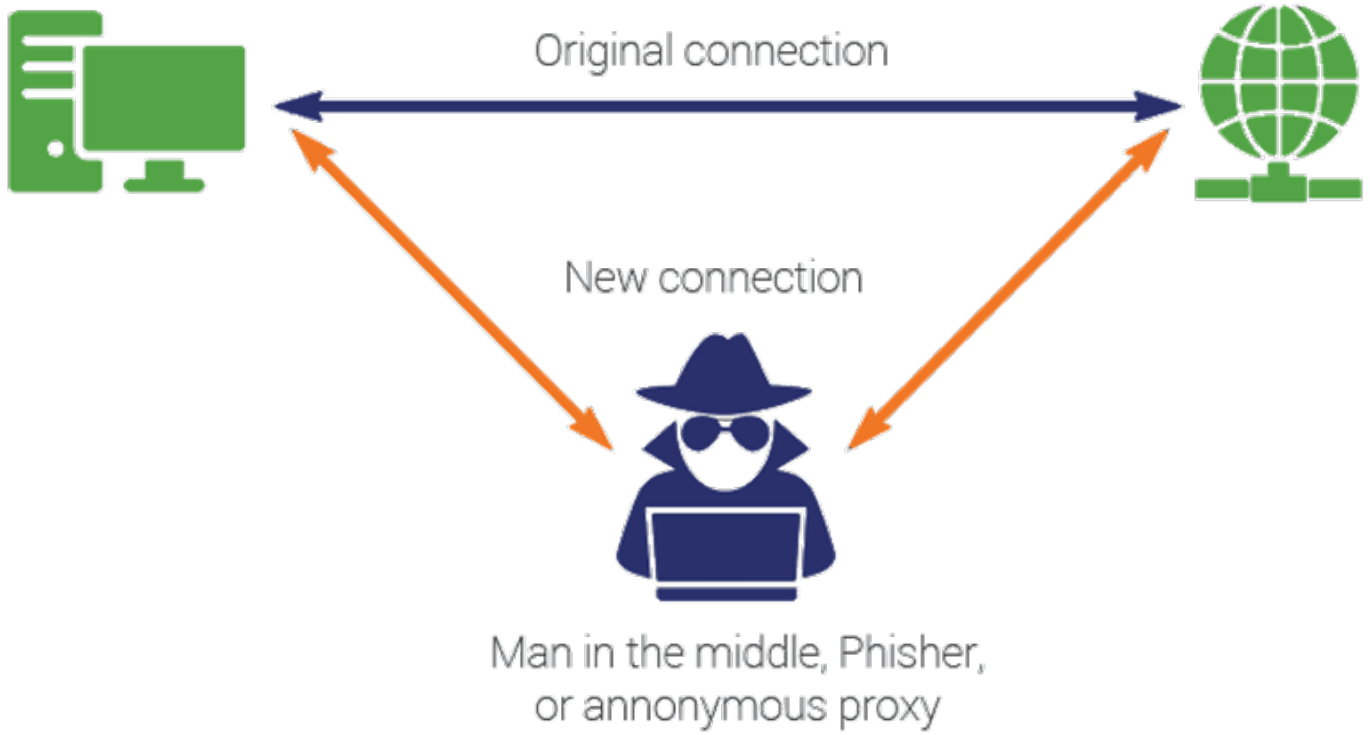
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

The clues about this phishing can be harder to spot

Ransomware attacks often start with a successful Phishing email.

Leading to a Man-in-the-Middle attack to gain access to the corporate systems

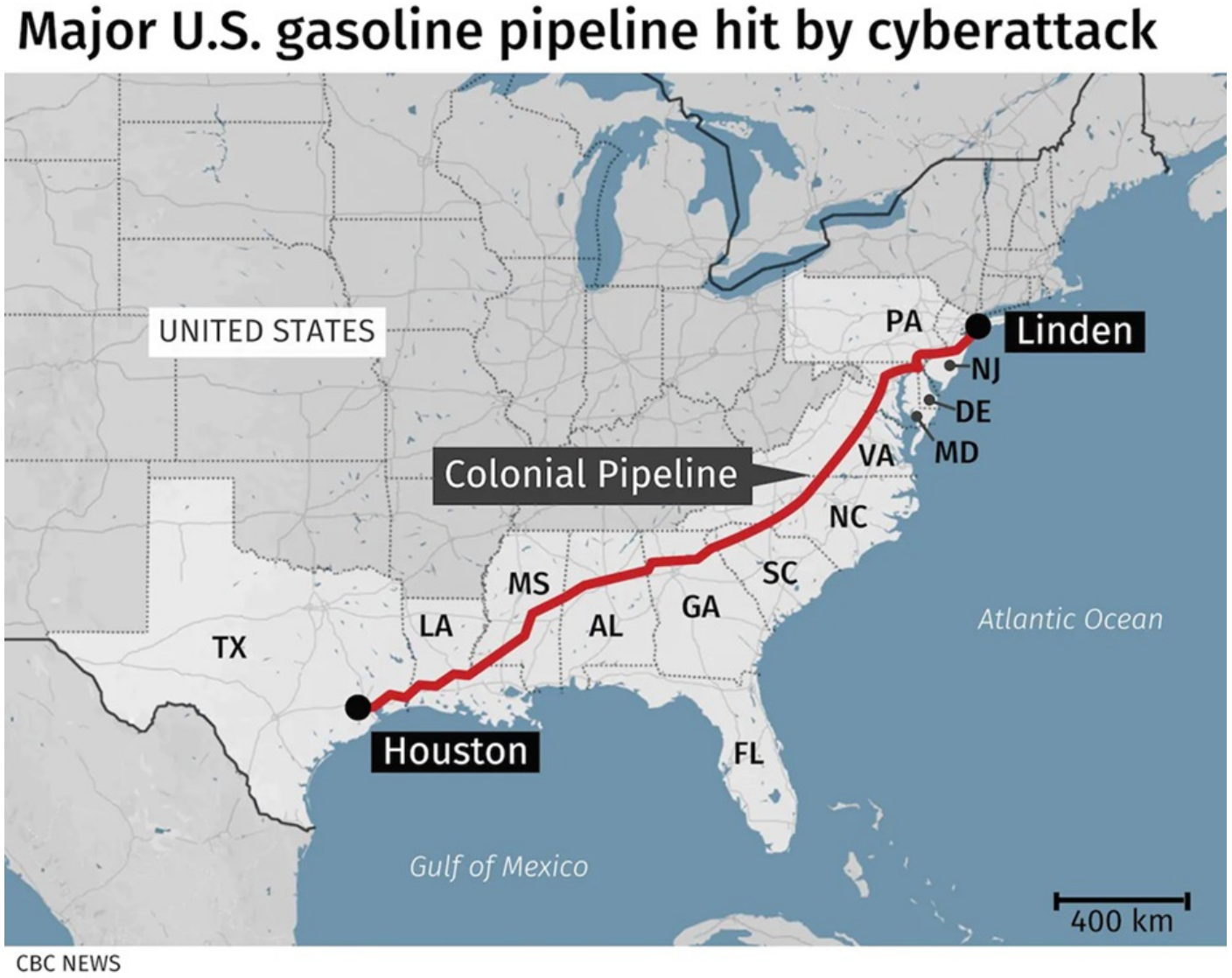


GTMARITIME

Colonial Pipeline Shut down for 6 days

Paid 75 Bitcoin (US$5Mill)

Because one Phishing attack was successful!



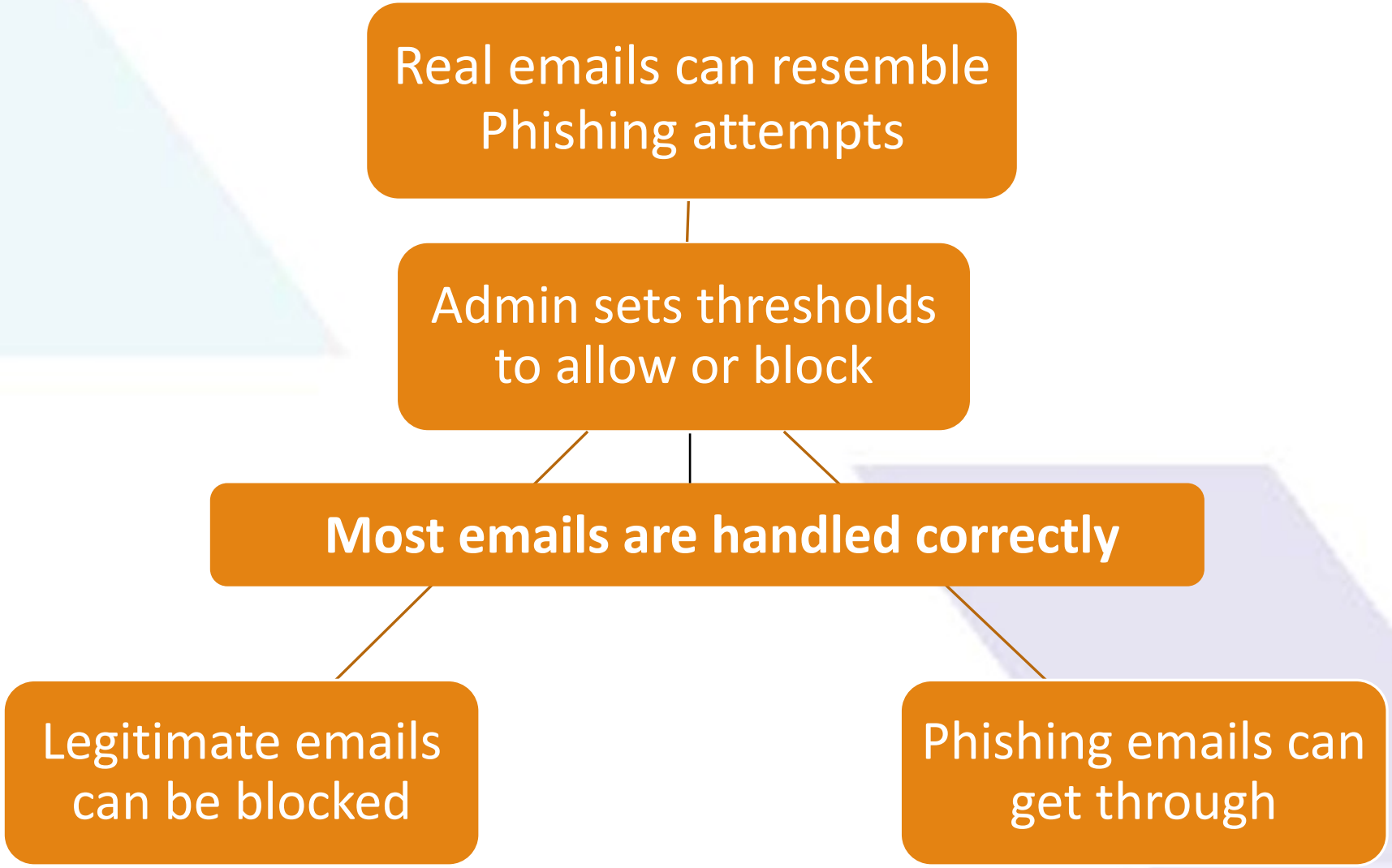
GTMARITIME

The Steamship Authority in Massachusetts hit in June.

Impacting the Ferry Service's Ticketing Systems

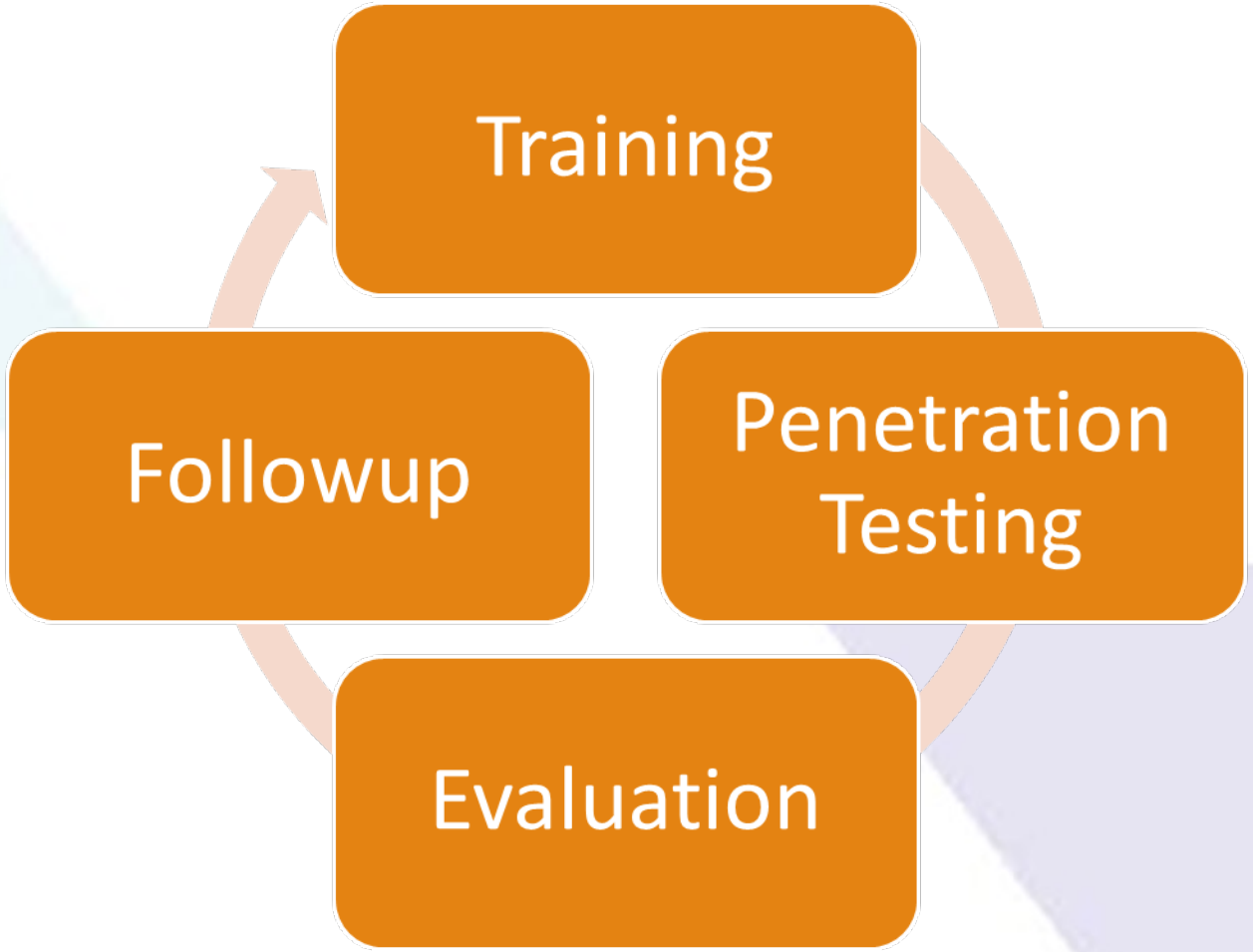
Click to add text

Anti-Phishing software cannot stop 100%



GTMARITIME

Office staff and crews must be vigilant!



GTMARITIME

GT Phishing Penetration Testing – the setup

- Three Phishing messages are created, using information readily available by public searching; i.e.
  - Port Authority – requesting vessel details via email
  - Port Authority – requesting crew details via a link
  - Mailbox Full – requesting login details

- One of these message is sent to each ship, bypassing the normal Anti-Phishing mechanism

GTMARITIME

GT Phishing Penetration Testing – the STING

- On avg. out of 1,000 vessels, sent a Phishing message
  - 124 respond with the requested information
  - Some provide all crew passport information
  - Others share their users emails and passwords
- The results varied widely by fleet. Training pays off
- In the worst case 50% of the ships in a fleet responded with the requested information

GTMARITIME