Key Takeaways

- By the end of this sessions you should:
  - Be able to recognize the changing landscape of business email compromise
  - A combination of people, process and technology is required to mitigate BEC

- Recognise key mitigation techniques, including:
  - Update Security Awareness Training and develop BEC Playbook
  - Build-in multiple person authorizations to approve significant wire transfers
  - 2FA to mitigate credential compromise
  - Monitor for executive over exposure online and domain impersonations

RSAConference2019
Asia Pacific & Japan

RSA®Conference2019
Asia Pacific & Japan

Business Email Compromise: in thematic context

Social Engineering and Account Takeover

Business emails in demand

- Contract scans

- Purchase orders

- Payroll information

- Financial reports

RSA Conference2019
Asia Pacific & Japan

Method 1: Social engineering

Reconnaissance on business and employees → Register fake domain → Send spoof email → Request transfer of funds → Target initiates transfer of funds

RSA Conference 2019
Asia Pacific & Japan

THE LOCAL it

News   Jobs   Community   Advertise with us   f ⤫ in ⌐

Lazio football club fell for a €2 million email scam: report

AFP
news@thelocal.it
@thelocalitaly

28 March 2018
17:07 CEST+02:00

football

sport

crime

lazio

Share this article

Cyber-Scammers Steal €50 Million from Austrian Airplane Manufacturer

FACC falls victim to a Business Email Compromise attack

Jan 21, 2016 13:55 GMT · By Catalin Cimpanu ⤫ · Share: ⤫ ⨍ ⬛ ⨁ G+

FACC Operations GmbH, an Austrian company that produces various airplane parts for companies like Airbus and Boeing, has announced a cyber-incident during which cyber-fraudsters managed to steal around €50 million from their bank accounts.

The company published a note about the incident on January 19, saying it was "a victim of a crime act using communication and information technologies."

FACC did not add anything more, except that the total damages were not yet fully accounted for, but the sum revolved around €50 million / $54 million.

Bloomberg

Technology

How One of Australia's Richest Men Lost $1 Million in Email Scam

By Kaye Wiggins
15 December 2017, 10:58 GMT *Updated on 15 December 2017, 14:55 GMT*

▶ John Kahlbetzer's administrator was tricked to make payment
▶ Man accused of involvement in the fraud says he's a victim too

SHARE THIS ARTICLE
Facebook
Twitter
LinkedIn
Email

In this article

● LIVE ON BLOOMBERG
Watch Live TV ›
Listen to Live Radio ›

The multi-millionaire founder of Twynam Agricultural Group Pty Ltd. lost $1 million in an email fraud, a London court heard Thursday. The British man who facilitated the theft says he's a victim too.

John Kahlbetzer, who is on the Forbes list of the 50 richest Australians, lost the money when fraudsters tricked the administrator of his personal finances into transferring it to them, his court papers say.

6
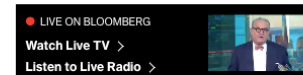
Method 2: Account compromise

RSA Conference2019
Asia Pacific & Japan
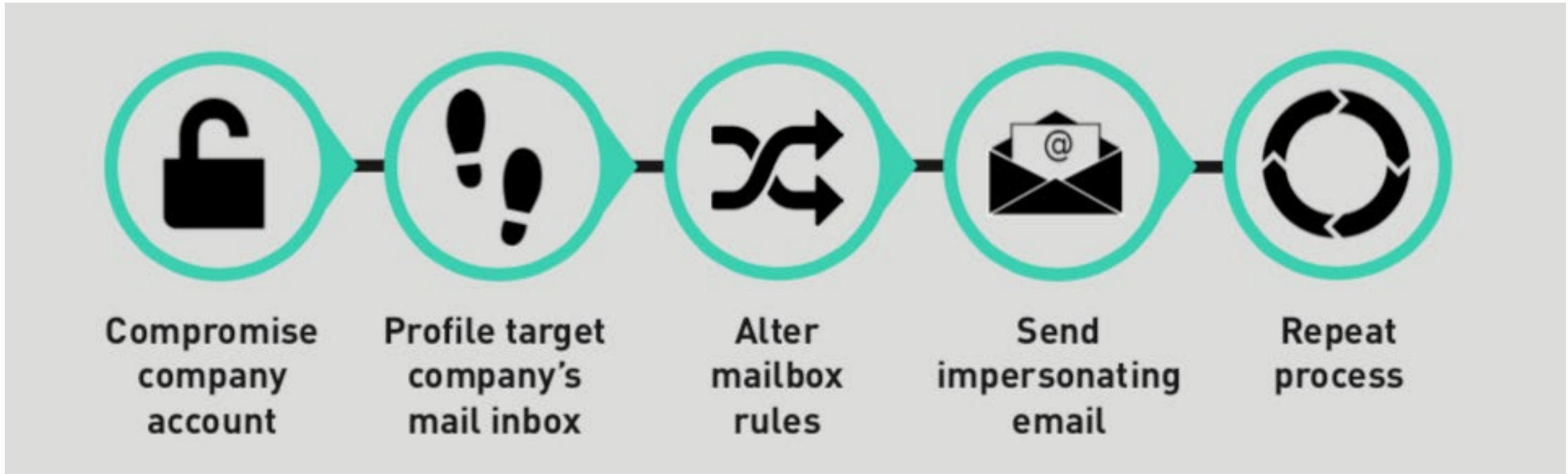
Co-operative bank's email hacked, Rs 95 lakh looted

TNN | Updated: Jun 3, 2018, 20:03 IST

BENGALURU: A private co-operative bank has alleged that tech-savvy criminals hacked into its official email and siphoned off Rs 95 lakh two transactions on May 28 and 29 from their account a IDBI Bank.

Cybercrime police of the Criminal Investigation Department have filed a cas against unknown persons based on a complaint filed by T L Hanumantharaya, chief executive officer, Sri Su Co-Operative Bank Ltd.

Representative image

THE STRAITS TIMES

SINGAPORE

ST | SINGAPORE | POLITICS | ASIA | WORLD | VIDEOS | MULTIMEDIA | LIFESTYLE | FOOD | FORUM | OPINION | BUSINESS | SPORT | MORE ▾

SINGAPORE › Courts & Crime | Education | Housing | Transport | Health | Manpower | Environment

Police warn against scammers alerting WhatsApp users to account takeover scams

RSAConference2019
Asia Pacific & Japan

8

Multiple Ways of Accessing Inboxes without Phishing

1. Paying for access

It's possible to outsource this work to online actors, who will acquire company credentials for a set fee or percentage of earnings. The price will vary depending on the type of mail service, but services are available from as little as $150.

2. Getting lucky with previously compromised credentials

It's common for employees to reuse passwords across multiple accounts. With many email and password combinations of finance departments email accounts already compromised, cybercriminals can get lucky.

3. Search across misconfigured archives

Why go to a dark web market when you can get sensitive information for free on the open web? With employees and contractors having to turn to easy, rather than secure, ways of archiving their emails, the barrier for cybercriminals is dramatically reduced.

RSAConference2019
Asia Pacific & Japan

Paying for Access: going out for tender

bosskel
Joined: 3 years ago
0 posts

Primary post
Hi I need fresh **Australia** and Europe business email and pass I am ready to buy. Please contact me on ICQ :678166154

Home > Buy, Sell, Trade, Services Offered / Wanted > Topic

[   ] Search

Advanced

Buying hacked company email accounts

Posted by JulieCash
Forum List Message List New Topic
JulieCash
Buying hacked company email accounts
August 02, 2018 04:56AM
Up to $5000 all via WSM escrow

Business/Corporate Email Hacking
asked Jan 20 in Hidden Answers by C

- email
- hacking
- database
- business
- corporate

RSAConference2019
Asia Pacific & Japan

Getting lucky with previously compromised credentials

- 437,746 finance department email addresses exposed in third party breaches

- 34,000+ APAC domains

- Searched for:
  - accounts@company.com
  - payments@company.com
  - receivable@company.com

Top Level Domain	Credentials Exposed
.com.au	20898
.in	5040
.co.in	3120
.co.nz	1707
.net.au	1018
.com.hk	743
.org.au	564
.com.sg	508
.comau	367
.tv	326
Total	**34291**

RSA Conference2019
Asia Pacific & Japan

BEC Goldmine

Searching Across Misconfigured Archives

RSAConference2019
Asia Pacific & Japan

2,326,558,731
files currently exposed online

50% increase
in file exposure since
March 2018
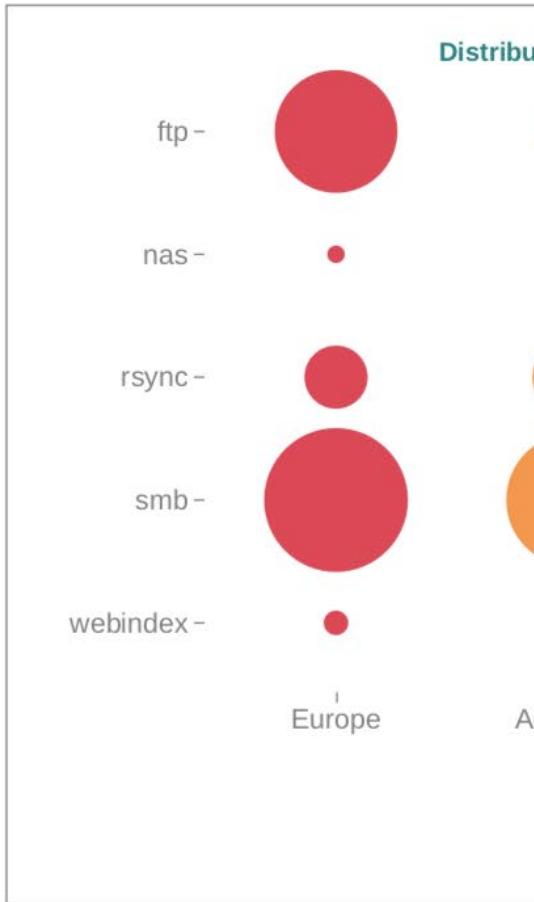
Region	File exposure
...urope	1,053,665,953
...mericas	590,056,298
...a-Pacific	399,300,440
...dle East	56,704,649
...frica	31,883,980
...ral Asia	1,189,421

Series1
77,314,533

ftp –
nas –
rsync –
smb –
webindex –

Europe   A

Distribu...

RSA°Conference2019
Asia Pacific & Japan

Singapore healthcare database hit by 'major cyber-attack'

James Walker 20 July 2018 at 15:00 UTC

Healthcare   Data Breach   Singapore

Data breach impacting 1.5m people was "deliberate, targeted, and well-planned"

Singapore

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.

Firms fined $1M for SingHealth data security breach

SingHealth and Singapore's public healthcare sector IT agency IHIS have been slapped with S$250,000 and S$750,000 financial penalties, respectively, for the July 2018 cybersecurity attack that breached the country's personal data protection act. The fines are the highest dished out to date.

By Eileen Yu for By The Way | January 15, 2019 -- 10:41 GMT (02:41 PST) | Topic: Security

SingHealth, the largest healthcare group in Singapore, has been the target of a "major cyber-attack" that resulted in the personal information of around 1.5 million individuals being compromised – including that of Prime Minister Lee Hsien Loong.

RSA Conference2019
Asia Pacific & Japan

Mitigating the Risk

1. Multi-factor authentication
2. Update security awareness training to include BEC scenario
3. BEC playbook
4. Work with your wire transfer application vendors to build in multiple person authorizations to approve significant wire transfers
5. Conduct ongoing assessments of your executive's digital footprints
6. Properly configure and authenticate file sharing services and NAS devices

RSA Conference 2019
Asia Pacific & Japan

RSA Conference2019
Asia Pacific & Japan

Key takeaways

Key takeaways

Many ways to access email inboxes
without phishing

1. Paying for access
2. Getting lucky with previously
   compromised credentials
3. Searching across misconfigured
   archives

RSΛConference2019
Asia Pacific & Japan

Key takeaways

- A combination of people, process and technology is required to mitigate BEC
  - Update Security Awareness Training and develop BEC Playbook
  - Build-in multiple person authorizations to approve significant wire transfers
  - 2FA to mitigate credential compromise
  - Monitor for executive over exposure online and domain impersonations

RSA Conference2019
Asia Pacific & Japan

Subscribe

- Download the report:

https://info.digitalshadows.com/BECResearchReport_Reg-Blog.html

- Subscribe today to get the latest information from Digital Shadows in your inbox

https://info.digitalshadows.com/SubscribetoEmail-BlogNews.html

- Check out our *ShadowTalk* weekly podcast

Pst! Cybercriminals on the Outlook for Your Emails

Authors: Rick Holland, Rafael Amado, Michael Marriott

digital shadows_

RSA Conference2019
Asia Pacific & Japan