S-RM | Atmos

Cyber Workshop

Interactive incident response simulation

unimutual

MARCH 2026

Today's Speakers

Mark Farley
Head of Proactive Services, APAC
S-RM Cyber

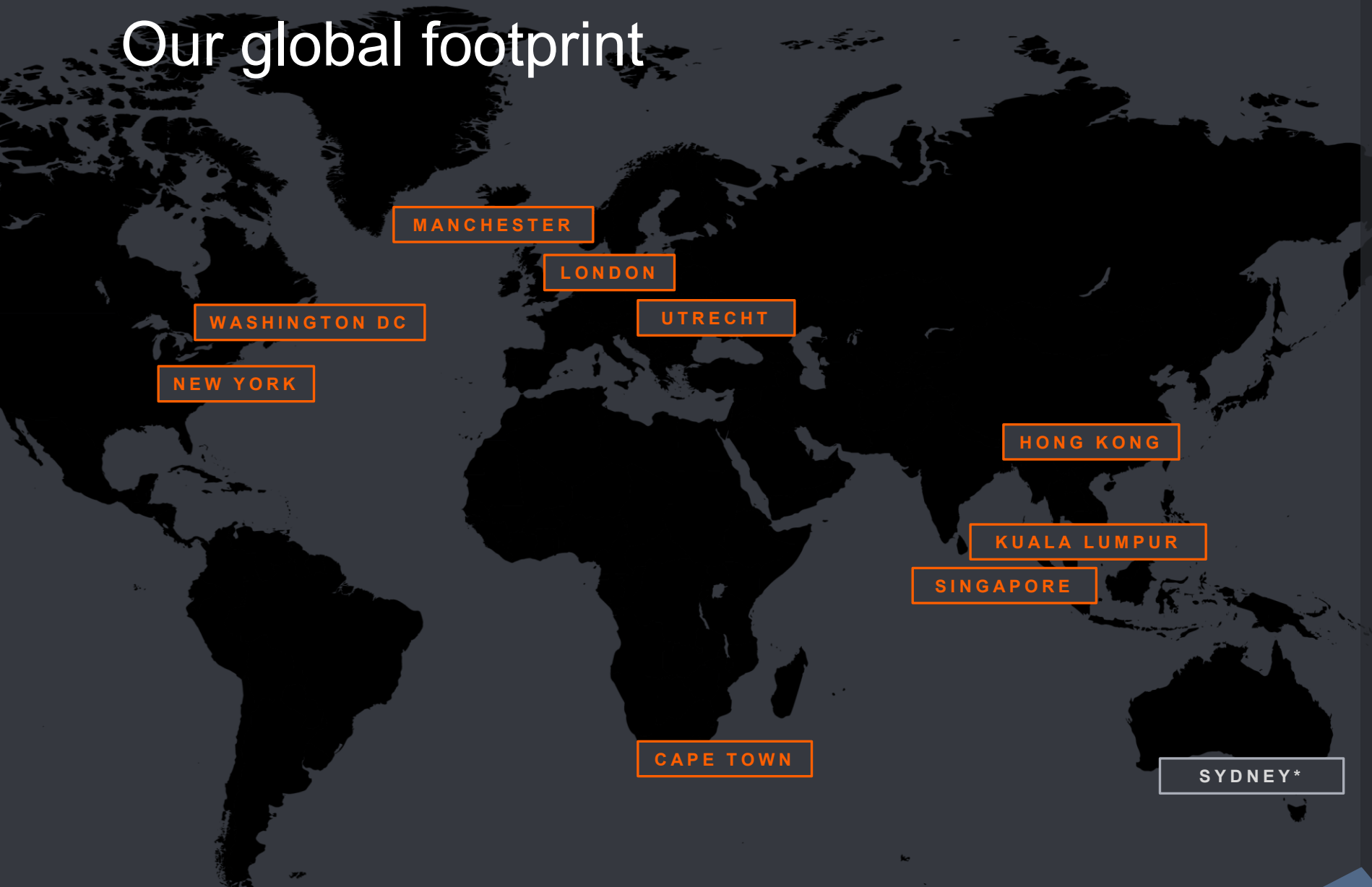
Will Stenmark
Senior Consultant
Atmos Australia & New Zealand

S-RM

S-RM is a global intelligence and cyber security consultancy

Our mission is to provide sharper thinking and superior service to our clients, always delivering actionable results.

Our global footprint



400+
Experts

45+
Languages spoken

Clients supported in
140+
Countries

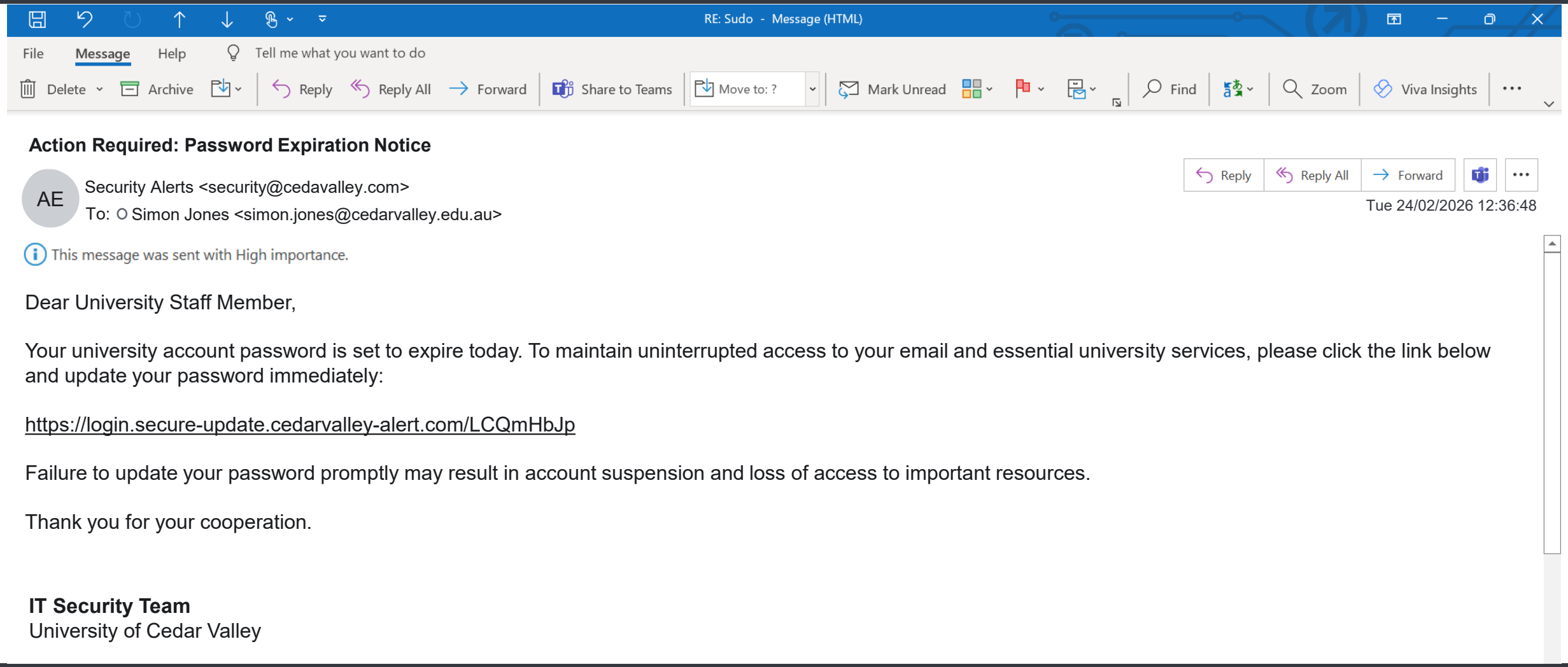
2005
Founded

9*
Offices globally

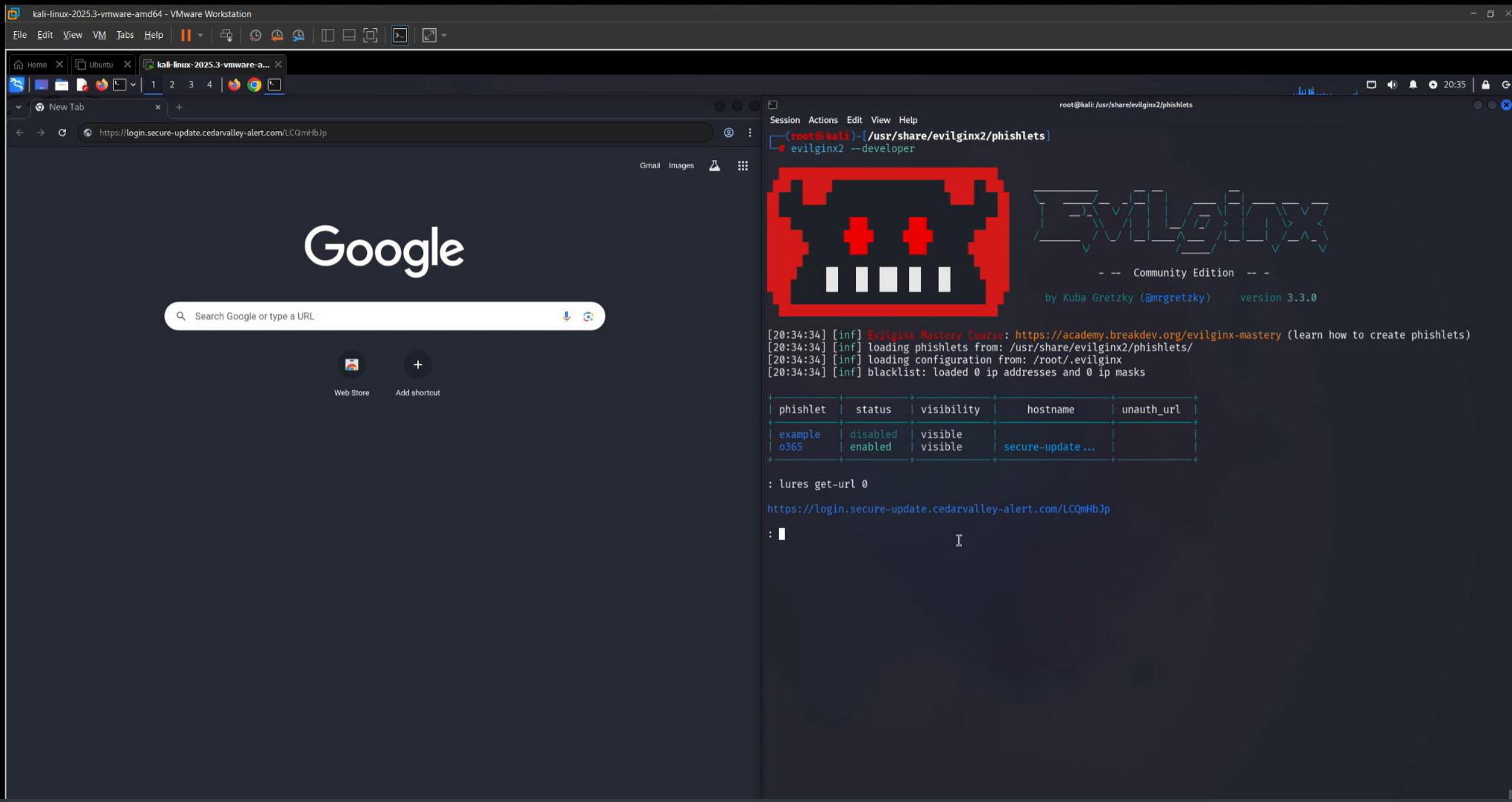
Join at slido.com
#2806934

Phase 1

Phishing email



What are the indicators that show this might be a phishing email?


kali-linux-2025.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu
kali-linux-2025.3-vmware-a...
1 2 3 4
20:35
New Tab
https://login.secure-update.cedarvalley-alert.com/LCQmHbJp
Gmail Images
Google
Search Google or type a URL
Web Store
Add shortcut
root@kali: /usr/share/evilginx2/phishlets
Session Actions Edit View Help
(root@kali)-[/usr/share/evilginx2/phishlets]
evilginx2 --developer
Evilginx
- -- Community Edition -- -
by Kuba Gretzky (@mrgretzky) version 3.3.0
[20:34:34] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[20:34:34] [inf] loading phishlets from: /usr/share/evilginx2/phishlets/
[20:34:34] [inf] loading configuration from: /root/.evilginx
[20:34:34] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
phishlet | status | visibility | hostname | unauth_url
example | disabled | visible
o365 | enabled | visible | secure-update ...
: lures get-url 0
https://login.secure-update.cedarvalley-alert.com/LCQmHbJp
:

Phase 2

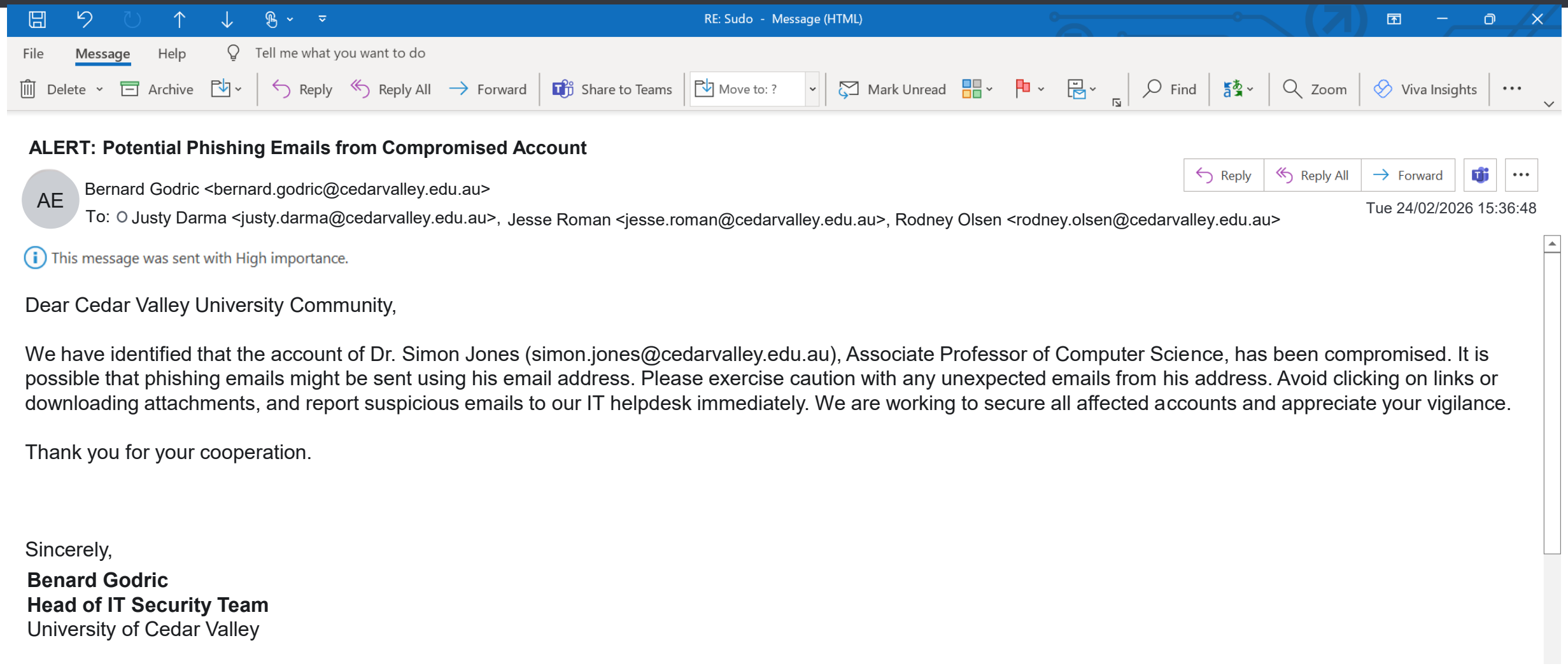
Mass phishing emails sent after first victim is compromised

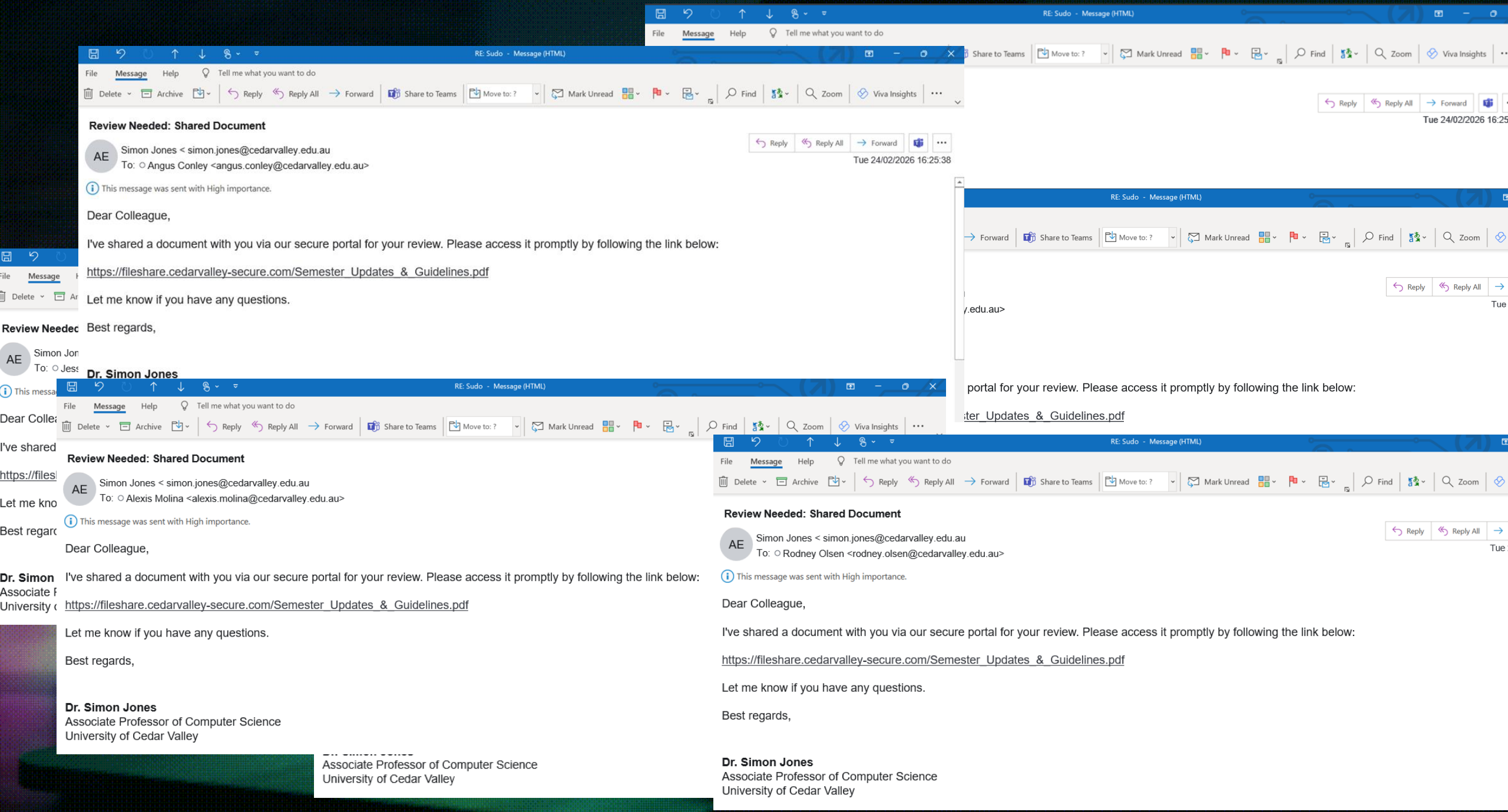
Using the compromised account, the attacker can send more phishing emails.

A user from your organization is now compromised. What steps would you take?

Phase 3

Impact of ransomware




RE: Sudo - Message (HTML)
File Message Help Tell me what you want to do
Delete Archive Reply Reply All Forward Share to Teams Move to: ? Mark Unread Find Zoom Viva Insights
Review Needed: Shared Document
AE
Simon Jones < simon.jones@cedarvalley.edu.au
To: Angus Conley <angus.conley@cedarvalley.edu.au>
Reply Reply All Forward
Tue 24/02/2026 16:25:38
This message was sent with High importance.
Dear Colleague,
I've shared a document with you via our secure portal for your review. Please access it promptly by following the link below:
https://fileshare.cedarvalley-secure.com/Semester_Updates_&_Guidelines.pdf
Let me know if you have any questions.
Best regards,
Dr. Simon Jones
Associate Professor of Computer Science
University of Cedar Valley
RE: Sudo - Message (HTML)
Review Needed: Shared Document
Simon Jones < simon.jones@cedarvalley.edu.au
To: Alexis Molina <alexis.molina@cedarvalley.edu.au>
This message was sent with High importance.
Dear Colleague,
I've shared a document with you via our secure portal for your review. Please access it promptly by following the link below:
https://fileshare.cedarvalley-secure.com/Semester_Updates_&_Guidelines.pdf
Let me know if you have any questions.
Best regards,
Dr. Simon Jones
Associate Professor of Computer Science
University of Cedar Valley
RE: Sudo - Message (HTML)
Review Needed: Shared Document
Simon Jones < simon.jones@cedarvalley.edu.au
To: Rodney Olsen <rodney.olsen@cedarvalley.edu.au>
This message was sent with High importance.
Dear Colleague,
I've shared a document with you via our secure portal for your review. Please access it promptly by following the link below:
https://fileshare.cedarvalley-secure.com/Semester_Updates_&_Guidelines.pdf
Let me know if you have any questions.
Best regards,
Dr. Simon Jones
Associate Professor of Computer Science
University of Cedar Valley

Situation update

Reports emerge that students and staff are not able to access their files and various learning platforms are not responding.

Your IT security team is deployed to investigate what is happening.

Your files and servers are encrypted, affecting your daily operations. How should you prioritise system restoration?

Phase 4

Notification obligation and reputation management

You have notified by the forensics team that data has been exfiltrated. What would you do now?

Phase 5

Engaging with the threat actor

README.txt

File Edit View H1

YOU HAVE BEEN HACKED!

What Happened?
We have encrypted your files using our LockGuardX ransomware. Your data, including critical academic and administrative information, is now inaccessible to you. Additionally, sensitive data has been exfiltrated and is stored securely with us.

How to Recover Your Data
To regain access to your files, you must obtain a unique decryption key. To receive this key, follow these instructions:

Deadline
You have 48 hours to complete the payment of 2 million USD. Failure to do so will result in the permanent deletion of your decryption key, making data recovery impossible.

Proof of Decryption
To demonstrate our ability to decrypt your files, you may send us up to 3 encrypted files. We will return them decrypted as proof.

Important
Do not rename encrypted files
Do not try to decrypt using third party software, it may cause permanent data loss.
Do not contact law enforcement or engage third-party recovery firms, as this will void our agreement and result in irreversible data loss.

Contact
For payment instructions and support, reach us at: l0ckcryptx2908h.onion

Your timely cooperation is crucial for recovering your data.

Ln 24, Col 1 | 1,171 characters | Plain text | 100% | Windows (CRLF) | UTF-8

Our Current Situation

BACKUP STATUS

Earliest known compromised is 7 days ago, but backup available only from 4 days ago

RECOVERY PROGRESS

Some issues with the recovery process means full recovery is estimated to take at least 21 days

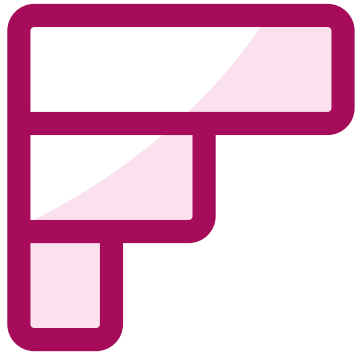
DATA LEAK THREAT

Threat actor threatens data leak in 48 hours if ransom is unpaid

RANSOM DEMAND

USD 2 million
48 hour deadline

The ransom note states you have 48 hours to make contact. What do you do now? Choose one option.



The executive board thinks the university needs to pay the ransom. However, the CFO and legal counsel are not so sure. Rank the top three factors for leadership to consider to reach a decision?

Payment - Decision-making Frameworks

Cost of no payment

- Breach of contract litigation
- Medium term Business Interruption
- Lost customers
- Potential regulatory fines
- PII data subject claims
- Rebuild costs

VS

Cost of payment

- Ransom amount
- Short term Business Interruption
- Low data subject claims
- Potential sanctions fines
- Lost customers
- Ethical/ Reputational impacts

Situation update

Backups are confirmed destroyed; unclear what data has been stolen.

24 hours since receiving the ransom note – with 24 hours left on the timer.

Forensics team says it will take more than the remaining time to figure out what data was stolen.

The executive board wants to pay a ransom.

Confidential © S-RM 2025

When should you make contact with the threat actor? Choose one option.

Who should communicate with the threat actor? Choose one option.

Key negotiation points

No decision makers should carry out the communication.

Introduce approval barriers and de-escalate pressure tactics with bureaucracy.

Most threat actor communications happen through **dark web sites** or **anonymous chat tools** that a specialist/technical expert will be comfortable using safely.

Threat actor chat portals are often monitored, drafting live in them can **give away your negotiation strategy.**

Situation update

Ransom demand confirmed – they want USD 2 million in Bitcoin.

They have **not** made good on their threat to leak data after you talked through the deadline.

The maximum the board is willing to pay is USD 600,000.

The board are also having second thoughts about whether they can trust the threat actor to honour any agreement if they pay.

How can you be sure that the threat actor will honour any agreement you reach? Select all applicable options:

Can you trust criminals?

Organised ransomware business models go after long-term revenues from many victims, which means they must establish a level of “trustworthiness” by honouring agreements.

Proof of possession and decryption and stolen data has become a common and relatively frictionless process that is accepted by most prolific ransomware groups.

Staging payments
with ransomware groups rarely works or is accepted.

Situation update

The proof of possession process is complete.

Negotiation on the price begins.

The threat actor has decrypted two sample files you provided to them.

The threat actor has also provided a file tree of stolen data.

What arguments might you use to convince the threat actor that you cannot pay their asking price of $2 million? Select all options you think would be effective:

Negotiations continue

The threat actor pushes back on arguments that you cannot pay USD2 million.

- They reply, saying that they have seen your financial statements from last year, and say you can afford it, but they can do a discount if you pay quickly.
- They ask for your offer.

In order to ensure the highest chance of a successful resolution, without exceeding a final asking price of $600,000, where should you start your initial offer?

Negotiations continue

The threat actor counter-offers $550,000, you decide to pay.

- They say while your sum is low, they have spoken to “the boss” and can make you an offer of $550,000, **but you need to pay now**.
- The board has decided to move forward with the payment.
- You do not hold Bitcoin.

What do you need to do before payment? Select all applicable options:

The threat actor fulfils settlement

You receive a decryptor via the threat actor's dark web portal.

The threat actor confirms they have deleted the data they stole.

They provide commentary explaining how they got into the network.

They state they will not attack you again.

Key takeaways

1. **Incident response and business continuity plans** are crucial for making correct decisions.

2. Accurate **threat intelligence** influences response and negotiation strategy.

3. Cyber response involves a consideration of **financial, legal, regulatory, reputational** and **ethical** concerns.

4. Establish **how you would make hard decisions** (such as paying a ransom) before an incident occurs.

5. Take legal advice to ensure your cost benefit analysis of a potential payment is the full picture. Remember, **you might still need to notify affected people if you pay**.

6. Above all, **cyber insurance** is a key risk transfer mechanism, and provides access to a **network of trusted and proven experts**.

For more information

Visit our website at www.s-rminform.com

Email us at hello@s-rminform.com

CONNECT WITH US ON SOCIAL MEDIA