An Australian Government Initiative

Regional Development Australia
SOUTHERN INLAND

Sasha Hajenko - CISSP

- 20+ years in IT/Cyber servicing private sector
- Businesses from 1- 1000+ staff, NGO/NFP
- Finance, construction, healthcare, legal, consulting, tech and more

Blue Phoenix Systems

Agenda

- Why everyone is a target for cybercriminals
- The Australian Cyber Security Centre “Essential Eight”
- Spotting a scam email or SMS
- Cyber Insurance and how it can help
- Resources to boost your awareness

Blue Phoenix Systems

A matter of not if but when!

- Defeatist and unhelpful phrase
- Don’t succumb to FUD or logical fallacies
- Use a risk-based approach

Blue Phoenix Systems

Cybercrime and SMB

- The SMB sector reported the most attacks
- Take sensible and strategic steps to improve your cyber resilience
- An ounce of prevention is worth a pound of cure
- Cybersecurity is a business issue, not a technical one

Blue Phoenix Systems

Types of attacks

- Majority of attacks are opportunistic, not targeted
- Email links and attachments are the primary threat vector
- Over 90% of reported attacks involved ransomware

Blue Phoenix Systems

The Essential Eight

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

[Essential Eight | Cyber.gov.au]

- Top Eight strategies to mitigate cyber incidents
- First developed in 2010
- Maturity Model – L0 to L3
- Essential = Baseline

Blue Phoenix Systems

Three Pillars

- Prevent malware delivery and execution
- Limit the extent of cybersecurity incidents
- Recover data and systems availability

Blue Phoenix Systems

#1 Application Control

- Pillar: Prevent malware delivery and execution
- Blocks anything except authorised (whitelisted) software from running
- Very high protection/High costs

Blue Phoenix Systems

#2 Patch Applications

- Pillar: Prevent malware delivery and execution
- Applications are the way we interface with data
- Vulnerabilities can be exploited to steal data or take control of systems
- High protection/Low costs

Blue Phoenix Systems

#3 Application Hardening

- Pillar: Prevent malware delivery and execution
- Applications come with many features, some can be used against us
- Turn off un-needed features and options
- High protection/Medium costs

Blue Phoenix Systems

#4 Office Macro Settings

- **Pillar: Prevent malware delivery and execution**
- **Macros can be very useful, can also deliver malware**
- **Turn off macros, or enable trusted locations/publishers**

  File > Options > Trust Centre > Trust Centre Settings > Macro Settings

- **High protection/Low costs**

Blue Phoenix Systems

#5 Restrict Admin Privileges

- Pillar: Limit the extent of cybersecurity incidents
- Admin privileges are used to configure computers
- Almost all applications today do not require these to run
- High protection/Low costs

Blue Phoenix Systems

#6 Patch Operating Systems

- Pillar: Limit the extent of cybersecurity incidents
- Patching is key to protecting your systems
- Windows 10/11 and Mac
- High protection/Low costs

Blue Phoenix Systems

#7 Multifactor Authentication

- Pillar: Limit the extent of cybersecurity incidents
- Something you know, something you have, something you are
- Stops 99% of account breaches – use passphrases if not available
- High protection/Low costs

Blue Phoenix Systems

#8 Regular Backups

- Pillar: Recover data and system availability
- Backups are your last line of defence
- Be strategic with your backup regime
- High Protection/Variable Cost

Blue Phoenix Systems

#8 Daily Backups cont.

- Determine your Maximum Tolerable Downtime (MTD)
- Test restoration to ensure your recovery time is less than your MTD
- Test at least one core system or process per year

Blue Phoenix Systems

Spot the Phish

- >90% of breaches start in the same place
- Well crafted, sometimes specifically targeting you by name
- A sense of urgency
- Build the human firewall

Blue Phoenix Systems

From: **DHL Express** (dhl@info.com)

Subject: **Shipment Arrival Notification**

Dear andy@attorneys.com,

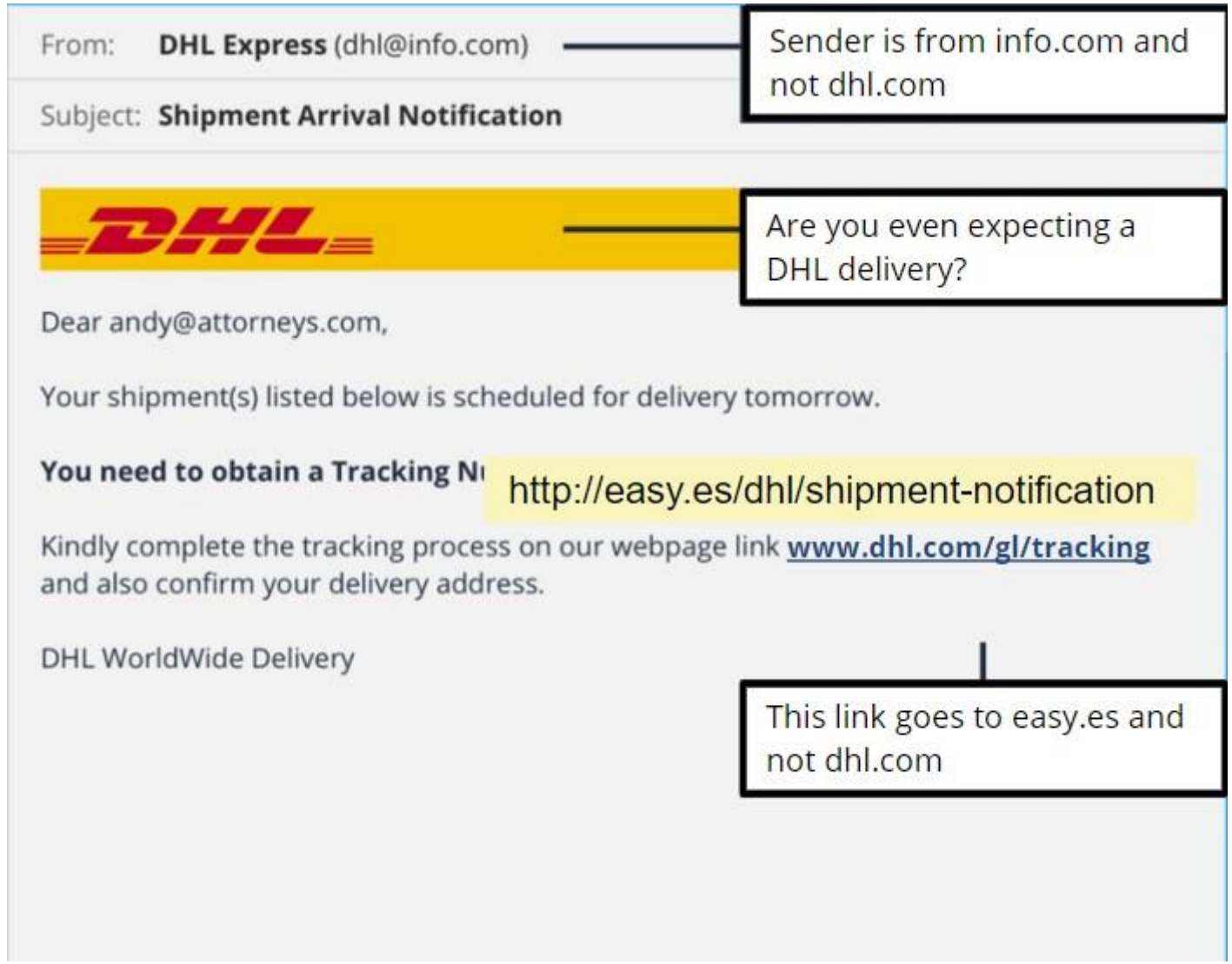
Your shipment(s) listed below is scheduled for delivery tomorrow.

You need to obtain a Tracking Number to check the status of the delivery.

Kindly complete the tracking process on our webpage link www.dhl.com/gl/tracking and also confirm your delivery address.

DHL WorldWide Delivery

Blue Phoenix Systems



Blue Phoenix Systems

Australian Government

Official Australian Government agency emblem

Our Reference: **14-A0-931C67** Monday, March 30, 2020 Subsidy benefit allocation

We are writing to bring to your knowlegde the allocation of your subsidy benefit.
Kindly affirm your eligibility by simply replying to this secure **message appropriately, as listed below.**

Please indicate correctly...

Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address *(Street number & name/Suburb/State/Postcode):*

Attach to your reply, a clear copy of your valid Australian Driver Licence **OR** Australian International Passport **and** a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | **Australian agency name and ABN**

Blue Phoenix Systems

Australian Government

Official Australian Government agency emblem

Our Reference: **14-A0-931C67** Monday, March 30, 2020 Subsidy benefit allocation

We are writing to bring to your knowlegde the allocation of your subsidy benefit.
Kindly affirm your eligibility by simply replying to this secure **message appropriately, as listed below.**

Please indicate correctly...

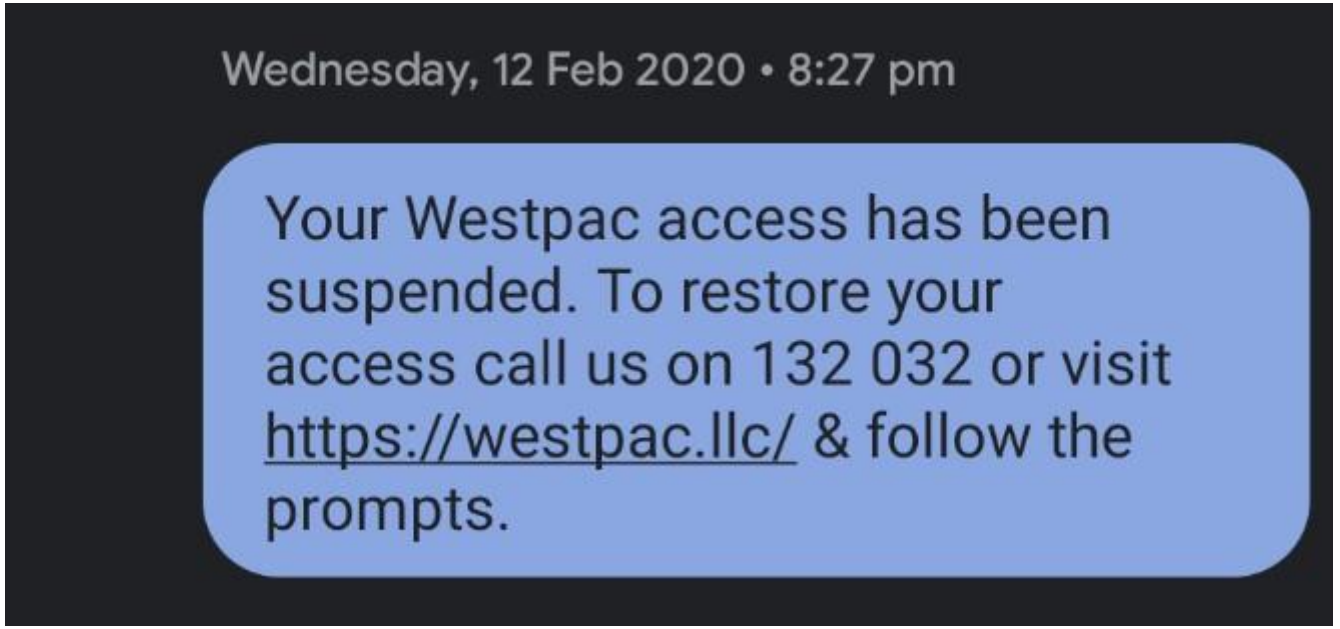
Given name (first only):
Family name/Surname:
Date of Birth (DD/MM/YYYY):
Tax File Number:
Complete Address *(Street number & name/Suburb/State/Postcode):*

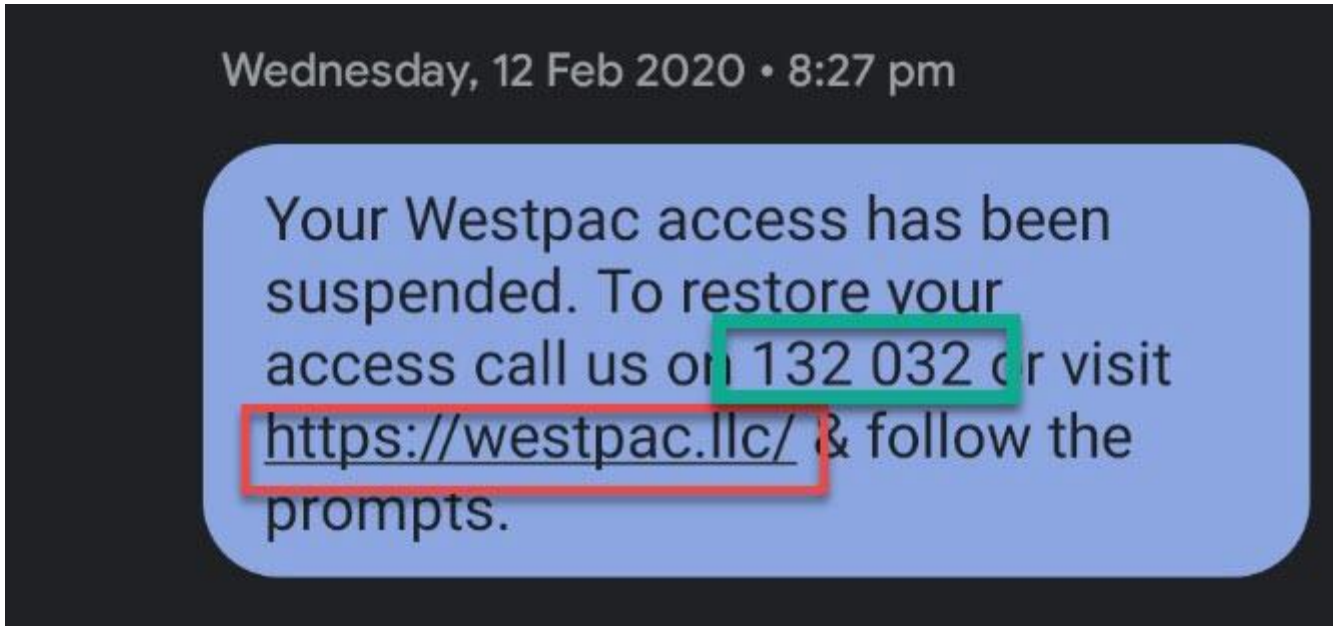
Attach to your reply, a clear copy of your valid Australian Driver Licence **OR** Australian International Passport **and** a clear copy of your valid Medicare Card.

©2020 Commonwealth of Australia | **Australian agency name and ABN**

Blue Phoenix Systems

Blue Phoenix Systems





Blue Phoenix Systems

Cyber Insurance

- Cyber incident response and recovery
- Obligations and mitigations
- Involve your insurer in your incident response

Blue Phoenix Systems

What else can I do?

- Understand and treat risk
- Identify your “crown jewels” and start there
- Think about your physical premises and how you protect it
- Technical and administrative controls
- Regular assessment and testing
- Continual improvement

Blue Phoenix Systems

Resources

Small Business Cyber Security

Small Business Cyber Security | Cyber.gov.au

Have I Been Pwned?

Check if your credentials have been released in a data breach

Have I Been Pwned

Have You Been Hacked?

How to tell if you have been hacked, and minimise the impact

Have you been hacked? | Cyber.gov.au

Blue Phoenix Systems

Questions?

Blue
Phoenix
Systems

www.bpsystems.com.au