



Cyber security micro-exercise report

Identifying and reporting a suspected phishing email

Prepared by: _____

Date: ____ / ____ / ____

Executive summary

Our team ran a discussion-based cybersecurity micro-exercise session on the reported date using the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) Exercise in a Box. This report summarises the results of this exercise and includes recommendations for our organisation to consider.

Discussion outcomes

What we learned from running the exercise:

How our understanding of preventing this type of cyber security threat changed:

What will we look to change or implement:

Team statements

We rated our confidence against the following statements:

	Not at all confident	Slightly confident	Somewhat confident	Fairly confident	Completely confident
We have regular and effective training in using peripheral devices (such as a USB drive) and how to identify suspicious links and unexpected email attachments.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
The information on our public social media and other online accounts is minimal, private and regularly reviewed to reduce the risk of becoming a target.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If we spot a phishing or fraudulent email, we have a clear reporting method to seek help and information.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
We have easily accessible policies and procedures in place in the event of a cyber security incident.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>