AusDBF Cyber Security Policy

Title	AusDBF Cyber Security Policy & Guidelines	**Policy No**	PN-0030
Version	2	**Date of Approval**	20/07/2021
Pillar area	Governance	**Schedule review date**	July 2023

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, the Australian Dragon Boat Federation *(AusDBF)* has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

AusDBF cyber security policy outlines our guidelines for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize AusDBF's reputation.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy Elements

Confidential Data Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of members/customers/partners and or vendors
- Patents, formulas or new technologies
- Customer and member lists (existing and prospective) and their personal details
- Employees' passwords and personal information
- Company contracts and legal records

All employees and volunteers are obliged to protect this data.

Protect Devices: When employees, contractors and volunteers use their digital devices to access AusDBF emails, data or Social Media accounts, they introduce security risk to our data. On this basis AusDBF instructs employees and volunteers to keep any device used to access that data secure. Ways to keep those devices secure are shown in the Guidelines

Protect Access to Company accounts: AusDBF uses many on line systems including Bank accounts, Accounting Software, RevolutioniseSport data portal and Office365. AusDBF instructs its employees who have privileged access to these systems to use industry best practice to help safeguard unauthorized access to them. Ways to do that are shown in the attached Guidelines.

Report Cyber Incidents:

Employees, contractors and volunteers are obliged to report any Cyber incident or breaches of AusDBF accounts to the AusDBF Finance Director

Keep emails safe

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, AusDBF instruct employees and volunteers to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Verify the legitimacy of each email, including the email address and sender name
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

Transferring Data Securely

AusDBF recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees and volunteers to:

- Avoid transferring sensitive data (e.g. member information, employee records) to other devices or accounts unless absolutely necessary.
- Share confidential data over AusDBF Office365 account and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

Additional measures

To reduce the likelihood of security breaches, we also instruct our volunteers and employees and to:

- Report stolen or damaged equipment as soon as possible to Business Services or Finance Director
- Change all account passwords immediately when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Guidelines to keep Devices and Data Secure

Top tips for protecting devices and access

- Use strong passwords and two-factor authentication and also change regularly
- For Bank accounts consider multiple authorisations for amounts greater than $2000
- Update your software
- Have antivirus installed
- Be careful of the information you share online that can easily identify you and be used against you
- Never click on suspicious links.

Strong passwords

A good rule of thumb for passwords is – the longer the stronger! Consider a password that contains:

- at least 8 characters (14 characters is even better!)
- at least one upper case
- one lowercase
- one numeric
- one special character (not the % sign).

When you set up a password you should avoid using details that can easily identify you – such as your own date of birth, street number, age, name etc. These are too easy to guess.

Passphrases

A passphrase is similar to a password but is often more difficult to break as it is a sentence that is unique to you but easy to remember. It is generally longer and more complex than a password and ideally contains an uppercase, symbols and punctuation.

An example of a passphrase might be your favourite meal or activity:

- OurCoachisbe5t
- Only1Coff33aday
- WepaddleonSaturday!

FAQ

Social Engineering, Phishing and Cyber Fraud

What is Social Engineering?

Social Engineering is effectively the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

A common example is where a person receives a phishing email which is a clever, authentic-looking email aimed at tricking individuals into disclosing sensitive information or carrying out tasks through deceptive means. They can include malicious links, attachments or redirection to a fake website that requests information.

The email looks like it has come from a legitimate sender such as your colleague, organisation, supplier or vendor.

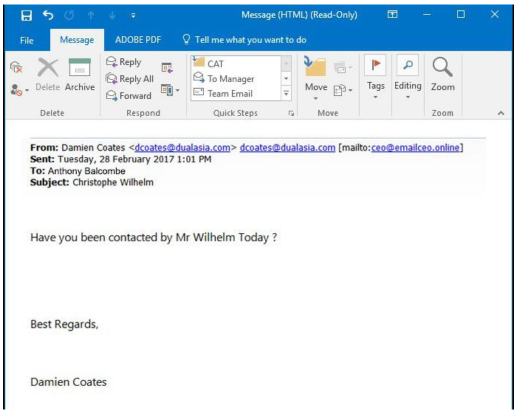
Aren’t scam emails blocked by junk mail or firewalls?

Even the most sophisticated email servers will allow some phishing emails to go through, so it’s important to check every request for payment or invoice received by email thoroughly before forwarding on for, or organising, payment.

How can you tell if an email is a phishing email?

You can often spot a phishing email from the following:

- The return and/ or reply email address are unknown to you or contain spelling errors. Beware that when using a mobile phone, the return address may not fully display.
- The content urges you to get in touch with a unknown third party.
  Example: to arrange payment for a Telstra invoice contact Bimeks
- There are spelling mistakes or formatting errors in the email
  Example: Invoice date15th Mai 216 or pleaseclickheretopay
- The content requests sensitive information which you wouldn’t normally need to provide to a supplier, or that they should already contain on file.
  Example: Please provide your credit card details

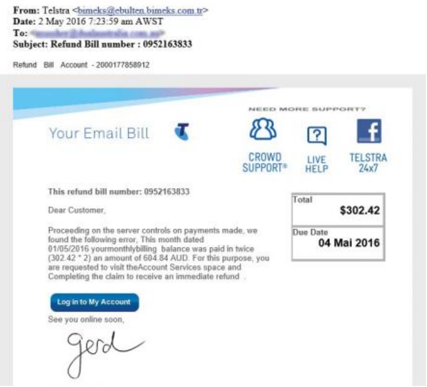


From: Damien Coates <dcoates@dualasia.com> dcoates@dualasia.com [mailto:ceo@emailceo.online]
Sent: Tuesday, 28 February 2017 1:01 PM
To: Anthony Balcombe
Subject: Christophe Wilhelm

Have you been contacted by Mr Wilhelm Today ?

Best Regards,

Damien Coates



From: Telstra <bimeks@ebulten.bimeks.com.tr>
Date: 2 May 2016 7:23:59 am AWST
To: [redacted]
Subject: Refund Bill number : 0952163833

Refund Bill Account - 2000177858912

This refund bill number: 0952163833

Total	**$302.42**
Due Date	**04 Mai 2016**

Dear Customer,

Proceeding on the server controls on payments made, we found the following error, This month dated 01/05/2016 yourmonthlybilling balance was paid in twice (302.42 * 2) an amount of 604.84 AUD. For this purpose, you are requested to visit theAccount Services space and Completing the claim to receive an immediate refund .

See you online soon,

gerd

Example: email (above) says it’s from Damien Coates
with return email ceo@emailceo.online

What if I receive a phishing email?

1. Do not respond or click on any of the links or attachments in the email
2. Forward the email to your IT service provider to confirm
3. Delete the email
4. Block the sender and warn any other recipients

How can I help prevent falling victim to phishing emails or social engineering scams?

1. Check every invoice or email thoroughly against the tips above to ensure you are confident it is a legitimate request for payment or information before sending on, or organising payment
2. If in doubt, forward the email to the service provider it came from to confirm.
3. Ensure Finance has the following controls in place that may prevent scam requests for payment from getting through:
   - Verify all new bank accounts by a direct call to the receiving bank to confirm it is a legitimate account, prior to being established in the accounts payable system
   - Verify all changes to existing bank account details (including routing numbers, account numbers, telephone numbers and contact information), by placing a direct call using only the contact number previously provided by the vendor/supplier before the request was received
   - Send all confirmations of banking changes requested by the vendor/employee/client to a person independent of the requestor of the change, with any changes being implemented only after the vendor/supplier could challenge them
   - Ensure there is a review of all changes to banking records by a supervisor or next-level approver before any change to the record is processed
   - Changing passwords for all online accounts and banking at least every 45 days and that the password protocols accord with industry best practice, or adopts two factor authentication;
   - Set up bank accounts so that payment amounts over $2,000 require a second co-signing authority
   - Run exception reports, either automatic, or manually created, showing all changes to the standing data of vendors/supplier

What is Phreaking?

Phreaking means the unauthorised and malicious use of the telephone system of the Insured which results in unauthorised charges or bandwidth costs which the Insured is legally liable to pay

What is Cyber Fraud?

Cyber Fraud means an intentional, unauthorised and fraudulent instruction to a financial institution to debit, pay, deliver or transfer money or securities, but was in fact fraudulently transmitted by a third party without the knowledge or consent of the Insured

References: V-insurance Group (DUAL Australia) Fact Sheet, www:BetterTeam.com, resources.workable.com/cyber-security-policy