Website FAQ statement

4 JUNE 2018

Incident notification

A statement from Southport Sharks' CEO

To our valued members, customers, employees, corporate partners, and wider Southport Sharks community.

We wish to notify you of an incident that has involved unauthorised activity on our systems.

On 9 March 2018, Southport Sharks experienced issues with its point of sale systems. Upon learning of this, we took immediate action to restore and re-secure our systems. In addition, we immediately commenced an investigation with the assistance of IT and Cyber Security consultants.

During the investigation, it was identified that we had been affected by 'ransomware', which is a type of computer virus, which resulted in the encryption of data contained on our systems. With further investigation, it was concluded by our IT and Cyber Security consultants that there was no evidence that any of the information contained on our systems was accessed.

Despite this, as a precaution, we have taken steps to notify all potentially affected individuals and corporate partners of this incident and how it may affect them.

We have set up this dedicated webpage to provide further information and mitigation tips, and a dedicated email mailbox (**support@southportsharks.com.au**), should anyone have any further questions.

We wish to apologise to all individuals and corporate partners potentially affected by this incident and reassure you that we take your privacy and the security of your data very seriously.

Thank you for your ongoing support of Southport Sharks.

Dean Bowtell

CEO, Southport Sharks

Frequently asked questions

Q: Have I been affected?

A: We have reached out directly to potentially affected individuals and corporate partners to inform them of this incident and specifically how it relates to them. Please check your email (including junk/spam folder), or be on the lookout for a letter from Southport Sharks. We have contacted you at your current or last known email / mailing address.

Although we have done our best to notify everyone directly, we confirm that you may be affected by this incident if you were, as at 9 March 2018:

- an employee – this includes current and past employees;
- a member – this includes current and past members, and junior social club members and their parents / guardians;
- an events / functions centre customer – this includes those who made an online booking or inquiry; or
- a corporate partner – this includes those that did business with, and were a creditor of, Southport Sharks.

We can confirm that any information first collected by Southport Sharks from 10 March 2018 onwards has not been affected by this incident and so any new employees, members, events/function centre customers or corporate partners from 10 March 2018 are not affected by this incident.

Q: Why are you notifying me?

A: Although our IT and cyber consultants found no evidence that any information was accessed, Southport Sharks are taking the steps to notify potentially affected individuals and corporate partners as a precaution.

Once we became aware of this incident, we immediately investigated its potential impact. Our number one focus has been to clearly identify who has been (and rule out who has not been) potentially affected by this incident, and also identify precisely what information was contained on our systems as at 9 March 2018.

We have informed those potentially affected by this incident as soon as we practicably could.

Q: What information may have been accessed?

A: We confirm that no credit card details, Tax File Numbers, or driver's license or other government issued identification documents are affected by this incident.

The information that may have been accessed depends on what information you provided to Southport Sharks prior to 9 March 2018, and varies from person to person. However, the type of information could include (if provided):

Affected individuals	Information
Employee	Name, Gender, Date of Birth, Address, Telephone Number, Email Address, Next of Kin, Employment Status, Membership Number, and Photograph.
Member or Events / Function Centre Customer	Name, Gender, Date of Birth, Address, Telephone Number, Membership Number, Email Address, and Company Details.
Junior Shark Member	Name, Gender, Date of Birth, Email Address, Address, Membership Number, and Parent / Guardian Details.
Corporate Partner / Creditor	Invoices and Billing Details including: Name, Gender, Date of Birth, Address, Telephone Number, Membership Number, Company Details, and Bank Account Number.

Q: What action do affected individuals and organisations need to take?

A: With the assistance of IT and Cyber Security consultants, Southport Sharks was not able to identify any evidence that any of the information contained on its systems as at 9 March 2018 was accessed.

We have worked with Australia's leading National Identity and Cyber Support experts, IDCARE, to assess the risk of harm that this incident may pose, as well as the steps that those affected by this incident could take to prevent any potential misuse of their information.

As a precaution we have outlined below steps that individuals and corporate partners affected by this incident can take to maximise the ongoing security of their information.

Individuals

1. Review and continue to monitor your financial and payment card account statements for any discrepancies or unusual activity. Contact your financial institution if you have any concerns.

2. Remain vigilant to telephone call, SMS and email phishing scams, and only respond to legitimate Southport Sharks communications. More information about phishing scams is available on the ACCC's website (https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing).

3. Remain vigilant to unauthorised requests to port your mobile telephone number to another provider. In most cases the first indicator of unauthorised porting will be your mobile phone unexpectedly losing coverage and going into SOS mode. If this occurs, contact your telecommunications service provider to confirm whether a request for porting has occurred, and if so, request a reversal. You should also contact your financial institution to temporarily suspend online banking. More information about this type of scam is available on the ACCAN's website (https://accan.org.au/hot-issues/1385-fraudulent-mobile-number-porting-and-identity-theft).

4. Ensure you have up to date anti-virus programs installed on your devices.

5. Review and continue to monitor your consumer credit report for any discrepancies or unusual activity. You can apply for an annual free credit report from each of the consumer Credit Reporting Agencies below. You can also request that a ban be put in place while you investigate further. Relevant contact details are below:

CREDIT REPORTING AGENCY	WEBSITE
Equifax	https://www.mycreditfile.com.au/products-services/my-credit-file
Dun & Bradstreet (now Illion)	https://www.checkyourcredit.com.au/Personal
Experian	https://www.experian.com.au/consumer-reports/
Tasmanian Collection Service	https://www.tascol.com.au/about-my-credit-file/

6. You can find additional guidance about protecting your identity by visiting the Office of the Australian Information Commissioner's website (https://www.oaic.gov.au/individuals/faqs-for-individuals/social-media-ict-identity-security/identity-security).

Corporate Partner / Creditors

1. Remain vigilant to 'business email compromise' scams, whereby a third party could issue an invoice that look like yours but with different bank account details, in an attempt to divert funds away from your organisation. More information about this type of scam is available on pages 22 and 23 of the ACCC's Scam Report dated May 2018 (https://www.accc.gov.au/system/files/F1240_Targeting%20scams%20report.PDF).

2. Contact your financial institution and let them know that your bank account details may have been accessed, and confirm whether there are any measures that they can put in place to secure your bank account.

3. Review and continue to monitor your financial and payment card account statements for any discrepancies or unusual activity. Contact your financial institution if you have any concerns.

4. Ensure you have up to date anti-virus programs installed on your devices.

5. Review and continue to monitor your organisation's corporate credit report for any discrepancies or unusual activity. Relevant contact details are below:

CREDIT REPORTING AGENCY	WEBSITE
Equifax	https://www.equifax.com.au/businesscreditexpress/reports/company-credit-report
Dun & Bradstreet (now Illion)	http://dnb.com.au/business.html

Q: What steps has Southport Sharks taken to improve security?

A: In addition to taking steps to restore the affected data and re-secure its systems, Southport Sharks is working with IT and Cyber Security experts to conduct a comprehensive review of its systems and processes.

Q: Has Southport Sharks notified the Office of the Australian Information Commissioner?

A: Yes. Southport Sharks has contacted the Office of the Australian Information Commissioner about this incident and will be working cooperatively with that office. You can visit the Office of the Australian Information Commissioner's website for more information (https://www.oaic.gov.au).

Q: Who do I contact for more information?

A: We understand that individuals and corporate partners potentially affected by this incident may have further questions. We have established this dedicated FAQ webpage and will be updating it if, and when, any new information becomes available.

We have also established a dedicated email mailbox (**support@southportsharks.com.au**) in case you have specific questions.

Q: I am not quite sure what some of the words in this notice mean. Can you explain?

A: We have prepared a glossary of some of the terms mentioned above just to help clarify their meaning a little better.

Glossary

Word	Meaning
Encryption	The process of locking up information or data so that it is no longer readable or able to be accessed.
Phishing	*Phishing* scams are attempts by scammers to trick you into giving out personal information.
Porting	*The process of changing your mobile telephone number from one service provider to another.*
Ransomware	A type of malicious software (computer virus) designed to block access to a computer system or data until a sum of money (ransom demand) is paid. Southport Sharks was able to restore its systems and data without having to pay the ransom demand.