pont3

What has happened?

On Thursday 6 October 2016, we, Pont3 detected unauthorised access to our third party external electronic mailing account, using a legitimate user account. The associated password was changed immediately and contact was made with the third party provider of the mailing service to seek further clarification on what had occurred.

The provider confirmed that someone had gained unauthorised access to this account and in light of this their security team temporarily suspended our account while the matter was investigated further.

As the investigation continued it was determined that some participant, volunteer and associate information was taken via ‘data exports’ by this unknown and unauthorised user.

We have been monitoring access since this initial breach and no further unauthorised access has been detected. We are working with our internal IT team and external security specialists to handle the breach and address any related issues.

We are also working with NSW Police to further investigate this matter as a priority.

When were participants informed?

Participants were informed on Wednesday 12 October 2016. Communication was not provided prior to this date, due to further discussion with the Third Party Supplier, NSW Police and Cyber Security Experts. We needed to confirm exactly which records had been compromised. As soon as we were in a position to provide participants,

volunteers and associates with accurate confirmation, all affected parties were emailed and information posted to the relevant event Facebook pages.

Did the information taken include financial information?

No financial information was taken. We do not hold financial information on this or any other database.

What steps have been taken?

We have changed the password associated with the user account that the unauthorised person used when we discovered the breach on Thursday 6 October 2016, and have implemented additional access controls. We are investing in internal processes and systems to reduce the likelihood of a breach like this happening again with our internal IT team and specialised security experts.

Do you think you will find anything else?

We are continuing to conduct a thorough investigation and we are committed to updating you on developments that could impact you. However, based on the data we know to exist in the compromised system, we can confidently state that no credit card information, passwords, or other security-related information has been accessed.

How can I be assured you are taking the steps to protect my information in the future?

We are investing in internal processes and systems to reduce the likelihood of a breach like this happening again with our internal IT team and specialised security experts.

What information was taken?

The information may have included names, mailing addresses, phone numbers and email addresses. Each affected party has been contacted by email from Pont3 (support@pont3.com) with the specific data fields that have been accessed in relation to their email address.

Was the data encrypted?

The data was accessed via a compromised user account, through the normal application interface. As such, data encryption would not have had an impact given the nature of this compromise.

How do I know if I was affected by this security breach?

A number of mailing lists related to Pont3 events including Sydney Running Festival, Electric Run (Aus.) Sydney Harbour 10k and 5k, Manly Inflatable Boat Race, Warrior Run and Pont3 newsletter subscribers have been

accessed. If your email address is associated with one of these lists that have been compromised, we will be in contact with you directly via email from (support@pont3.com) with the data fields that were captured.

Pont3 attempted to contact all affected parties by email on Wednesday 12 October 2016.

Why do we use a third party provider for the distribution of its event related and marketing communications?

Many organisations utilise the services of a third party mail service due to internal systems not have the capability of managing bulk email deliveries. The use of third party mail systems also help deliver email more successfully to intended recipients.

Why was this level of information added into the third party external electronic mailing account?

We collect personal information in order to properly and efficiently carry out specific functions including; registration processes for events, provide you with key event information, requested products and services, as well as to facilitate and deliver targeted communications dependant on factors such as event, age, gender, location etc.

What does it mean if my information was stolen? What are the risks?

The primary risk is increased exposure to consumer scams, such as phishing, web scams and social engineering. We want to help our participants protect themselves by providing information and resources about these scams. For helpful tips and advice on online safety please visit www.staysmartonline.gov.au or www.iDcare.org

I have received a call, SMS or email from someone who said they were from Pont3 asking me for financial and/or other personal information. What should I do?

Do not provide this information. Be wary of scams that may appear to offer protection but are really trying to get personal information from you.

What kind of scams do I need to watch out for?

Following an event like a data breach it is common to see scammers use emails, SMS, phone calls and fake websites to try to access further personal information. The following are types of scams, scammers and terminology that may be helpful:

- **Social Engineering:** Using fraud or deception to manipulate people into performing actions or divulging information that they would normally not share.
- **Social Engineer:** A scam artist who contacts individuals via phone, email, text message or even in person to gather information for the purposes of fraud, data system access, identity theft and more.

- **Phishing:** A social engineer uses a fake email to trick recipients into giving up credit card information, passwords or other sensitive information. The email may appear to come from a trusted source, such as a reputable company or bank, and often includes personal details so it appears the sender knows you.
- **Smishing:** Similar to Phishing (see above), a social engineer sends a fake Short Message Service (SMS) text message to your cell phone, announcing that you've won a prize or offer from a trusted company or bank if you follow a link to a website and enter a code. Clicking the link can expose your phone to malware.
- **Pretexting:** When a social engineer impersonates someone with authority and creates a fake scenario to trick unsuspecting individuals into sharing private or sensitive information.

What are some things I can do to avoid social engineering scams?

Don't respond to SMS or emails received from a contact you don't recognise, and don't click on any included links. Instead, if you need to make contact with the organisation, directly type the website address you want to visit into your browser or look up their telephone number or email address.

Don't send money to strangers; scam artists often insist that you wire money, especially overseas, because it's difficult to trace the transaction.

For further tips as how to protect your security please visit www.idcare.org or www.staysmartonline.gov.au

What can I do if I think I have been scammed?

Please contact iDcare 1300 432 273 or contact the Australian Cybercrime Online Reporting Network www.acorn.gov.au

---