Friends of the
Australian National Botanic Gardens

Friends of the Australian National Botanic Gardens Inc.
GPO Box 1777, Canberra ACT 2601 • ABN 57 096 639 836
**p** 02 6250 9548 • **e** info@friendsanbg.org.au • **w** www.friendsanbg.org.au

# Important message for members of the Friends

## Intrusion into the Friends web server

The security of the server that hosts the Friends website and our membership database has recently been compromised, and unauthorised intruders have been detected.

**SUMMARY**

- Our website, membership database and other systems were temporarily affected, but have now been restored and all our data is safe;
- Some membership information (but not financial information) might have been visible, but we cannot know whether it was accessed. No banking or credit card details were involved, as these are not entered on to the membership database;
- Currently one intrusion is still periodically re-occurring, but is being manually detected and neutralised when it appears.

**WHAT MAY HAVE BEEN AFFECTED**

Initially, the intruders used a recently-discovered vulnerability in the widely-used Drupal software used by our website. They could then gain access to all files on the server.

We know that, as a result:

- the Friends website was interfered with and briefly became unavailable;
- the site description provided to search engines (such as Google) was temporarily replaced by false information;
- malware programs were placed on the server to generate spam emails, and possibly to 'mine' cryptocurrency;
- malware was also placed on the site to permit the intruders to gain access in future, even if the initial vulnerability was fixed.

The methods used, which seem to have been automated 'bot' programs rather than hands-on hacking, suggest that the intruders did not specifically target the Friends and had no particular interest in the content of the files they had access to.

We do not know whether information on the server was accessed or copied by intruders. It seems unlikely, but cannot be ruled out. The information accessible to them would include:

- the names, addresses and contact details of Friends members;
- receipts issued by the Friends for membership subscriptions and donations.

**OUR RESPONSE**

As soon as the Friends became aware of the intrusions:

- all Friends data was backed up;
- the Drupal website software was updated to remove the initial vulnerability;
- all files were checked, and those identified as malware were deleted or repaired;
- we began more closely monitoring all server activity.

**WHAT IS SAFE**

Our website has been scanned for malware, and none found. We do not believe there is any threat to people visiting the website.

No records of bank accounts, credit cards or similar sensitive financial information are kept on the server. Such information is safe.

No credit card processing, online or otherwise, was affected. All card transactions (such as donations to the Public Fund of the Friends) are undertaken by financial institutions using encrypted secure communications, which bypass our server and have not been breached.

Emails to or from Friends volunteers using '…@friendsanbg.org.au' forwarding addresses are not stored on the server. The content of such emails could not be accessed by the intruders.

**CURRENT SITUATION**

Ongoing monitoring has shown that one intruder can still place malware onto the server. This might be through 'backdoor' access, or perhaps because a yet-undiscovered source program installed earlier is still there and periodically generates new copies of malware files.

When re-infection occurs we can quickly detect it and delete the rogue files involved. After cleaning, our website and programs operate normally, and our data is not affected.

However, the ongoing re-infection shows that we have not yet fully regained control of the server, and this is a major concern. We are seeking specialist advice on how to counter this.

**FURTHER INFORMATION**

We will advise members via our website as soon as the server has been fully secured, and if any other significant development occurs.

If you have questions about what has happened and how you might have been affected, please email info@friendsanbg.org.au or call (02) 6250 9548 and leave a message. Please do not direct queries to the Membership team.

We will provide updates and respond to queries as soon as we can, but please understand that our priority at this stage is to fully restore and secure our services and data.