

GDPR and Cyber Security Guidelines for Treasurers

As a treasurer it is likely that you could receive scam or “phishing” emails from scammers trying to extract money unlawfully from our organisation. To help you spot and deal with this appropriately please follow these guidelines

- 1) If you receive an email asking you to transfer money or provide financial information, whether it seems legitimate or not, please phone the person who you think the email is from with the contact phone number you have for them. If you do not have a phone no for them contact head office. Do not reply to the email or attempt to transfer funds.

2) Three Common ways Scammers get in contact

- They send an email that looks like it has come from someone you know but it actually from a suspicious email address Please see image below. This is a real email that looks like it was coming from someone within the NGS, but on closer inspection you can see it is from a suspicious email address. It looks very genuine but it was not sent from George Plumptre our CEO but from a scammer.

From: George Plumptre <presidentialprivate.email@gmail.com>
Sent: 11 April 2018 10:10
To: Helena Pretorius <helena@ngs.org.uk>
Subject: National Garden Scheme Financial Report

Good Morning Helena,

I trust this email finds you well, I need you to set up a bank transfer payment, do you have few minutes to process the transaction today,

I will send you the banking details upon request, can you please send me the recent financial report at your earliest convenience.

Best,

George Plumptre
National Garden Scheme
East Wing Hatchlands Park
East Clandon
Guildford Surrey
GU4 7RT

-
- However, scammers are getting more sophisticated and can produce email addresses that look very genuine and that include names, so **if they are asking for money or for financial information about our organisation, double check first.**
 - It is also possible that a hacker could gain access to a legitimate NGS account and send out spurious requests, so in all cases **if you are requested to transfer money or share financial information PHONE FIRST AND DOUBLE CHECK**
- 3) Please from now on, as an added safeguard, can you always use your ngs.org.uk email address for National Garden Scheme business. If you do not have one set up contact head office who can arrange this for you. We can offer more protection to you from scammers if you do this including deleting and blocking known scam email addresses.
 - 4) If you do not currently have an ngs.org.uk email address or are at any time unsure, forward any suspicious emails to either joanne@ngs.org.uk or helena@ngs.org.uk and we can advise.

- 5) If you are sending emails out to groups of people please always blind copy the recipients (bcc).

Please, do not worry about offending anyone or seeming silly for double checking. Scammers are getting more clever in their tactics and it is better to be safe than sorry.

If you feel you have received a scam email

- Forward to head office, do not reply.
- Block the sender and check that their email address hasn't been remembered in your system as a contact for who they are pretending to be.
- Change your password
- If you have replied to the email or sent any details of our organisation to a scammer, or if you feel they may have gained access to your computer please refer to our document What to do if you suffer a data breach and **contact Head Office immediately**.

We advise that all members of County Teams use an ngs.org.uk for NGS business as we can protect you better from scams that way. If you do not have an ngs.org.uk email address please let head office know. However we cannot totally prevent scam emails, so awareness and double checking is key to stopping any potential breaches.