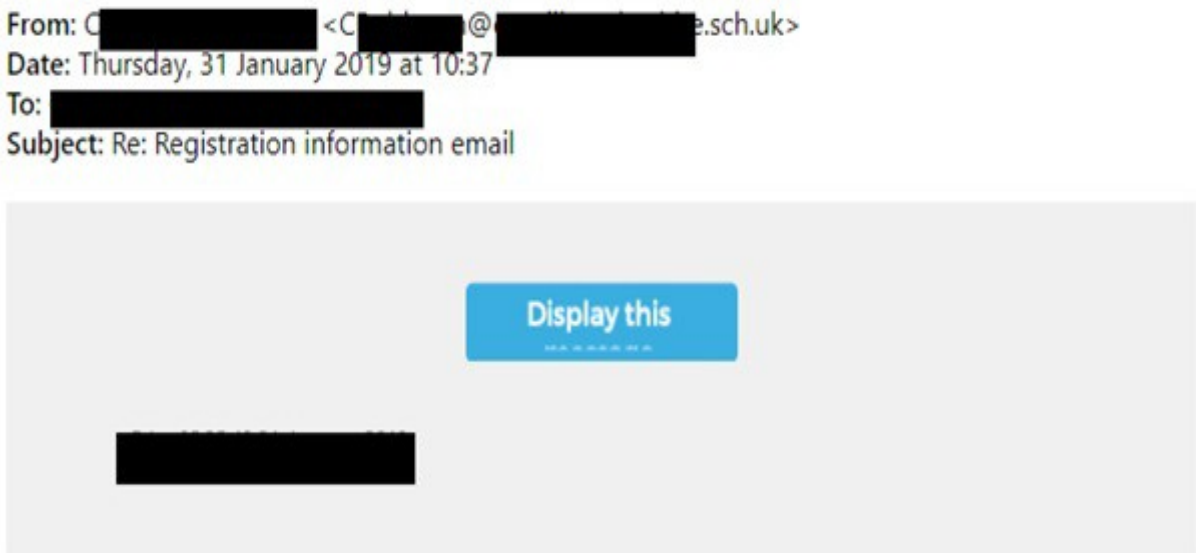
IMPORTANT DATA SECURITY UPDATE

Below is some guidance produced by DCC in conjunction with GDPR in Schools (GDPRiS), on how to handle these events and how to better protect yourselves in future.

The information below should be read by your Data Protection (DP) Lead/Data Protection Officer (DPO), your IT Support and it is advised that Senior Leadership are fully informed.

If you are using our DPO service, it lets us know immediately if you have received suspicious emails.



Here's what to do if you think you have been affected by a phishing email:

1. Identify which accounts have been affected and warn staff not to click on links they are not sure about. Get them to speak to the DP Lead/DPO, not just the IT Support Staff/Provider.
2. Log the breach in line with your breach reporting process. Guidance on data breaches can be found on SchoolsNet.

NB remember to update it with commentary on actions and findings.

3. Speak to your email and/or broadband provider as they may have already taken action or be able to help in your investigation.
4. Speak to your IT Support Services provider to assist you in identifying the nature and the extent of the attack and to help you understand anything contained within this advice note. You are welcome to contact our IT Support Services for Schools Manager Paul Livingstone who will be happy to assist. Mobile: 07795238237

5. Check compromised accounts for any issues relating to other systems/services. Also, warn affected staff to change personal account details if they use that password for personal shopping, etc.
6. Check whether any personal data is affected and determine if you need to report to the Information Commissioners Office (If we are acting as your DPO we will work with you to decide this).
7. Don't panic. Even the best of us are affected by phishing scams, which are getting harder to spot by the day. Review **ALL** the guidance included below and included in the links provided. Forewarned is forearmed!

Measures that can be taken on your account to mitigate this from reoccurring include:

- Reset of your password (strong password and one that shouldn't be used on other personal systems)
- Limiting the capabilities of connecting into your mailbox (removal of client applications from the list of email apps)

- Enabling Multi-factor authentication on the compromised account
- Further information can be found on the Microsoft website.

Useful Resources:

- The National Cyber Security Centre (NCSC)
- The Association of Network Managers in Education (ANME)