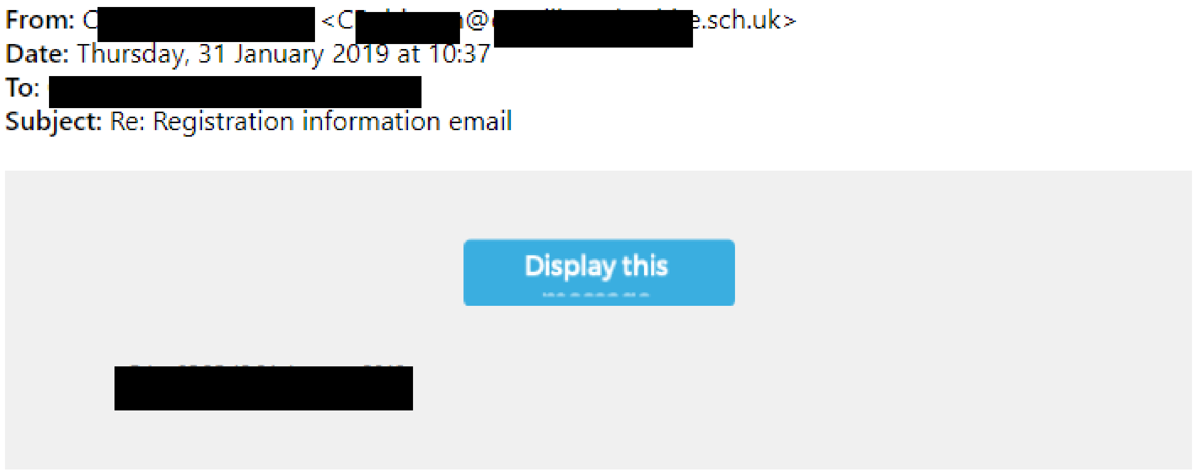
Phishing Scams In Schools aka "Click here to hand over your data!"

Data Protection and Privacy is not just about the issues with Facebook or people losing unencrypted memory sticks, it is also about protecting access to systems and services within a school. Passwords may be as strong as you like but if you unwittingly hand it over to someone, then you have still lost control.



From: [redacted] <[redacted]@[redacted].sch.uk>
Date: Thursday, 31 January 2019 at 10:37
To: [redacted]
Subject: Re: Registration information email

[redacted]

Example Phishing Email

This, unfortunately, is one of the issues affecting schools across the UK right now. A major phishing[1] scam started earlier in the week and is now reaching a significant number of schools. The team at The Association of Network Managers in Education (ANME) have written about the technicalities of protecting your school against it and we heartily recommend that you review this and pass to your IT support team and/or your IT support provider. Their article also includes the link to the EduGeek.net discussion on protecting your school.

The risks to schools with phishing scams are numerous. In this case, the aim appears to be to get as many credentials as quickly as possible, and to compromise those accounts. As so many schools now use cloud services where a single username and password can access multiple areas, this creates a risk, but a manageable one. That account may be linked to online storage; to filtering and monitoring systems; where there is administrative access on the MIS; be re-used on financial systems; be re-used for personal shopping accounts … it goes on. Once a password is compromised, you need to change it *everywhere* it might be used.

Let's see what you need to do to prevent this. As well as the guidance from ANME, you also need to give early warning to your staff. The National Cyber Security Centre (NCSC) has good advice on the approaches you can take but the important thing is to make sure staff are aware there is an increased risk at the moment, that they should be careful about clicking on any link to access more information, and if they have been affected, they should let the appropriate person know immediately. Whilst the initial thought of most people is that it's only the IT support staff/provider that they need to information,

[1] Phishing - https://www.ncsc.gov.uk/phishing#what

it's actually the DPO/DP Lead in the school that also needs to know immediately. If that is you, make sure that staff know who you are and how to contact you.

Contact your email provider and/or broadband provider, as they may be able to help you take preventative action or might have even already taken it by blocking connecting IP addresses/rogue machines, collating information to pass to authorities and so on.

The definition of a Personal Data Breach is *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data."*[2]

The main risk to personal data comes from the fact that accounts may be compromised and face further attacks. If this has affected your school, some additional investigation is likely to be needed. Here are a few of the questions which schools need to ask themselves:

- Have any of the compromised accounts got access to areas where personal data is held?
- Are you able to check if they have been accessed over the last few days?
- Has the access come from outside of the school and from an unexpected location?
- Are you able to check if anything has been downloaded or accessed?

If you have answered 'Yes' to most of these questions, then you may have a **reportable** data breach on your hands; there is a risk to people's rights and freedoms. But don't panic - GDPR in Schools customers should log the breach in their Breach Management section. Log the actions you have taken to mitigate further issues and log what you are doing during your investigation. Within 72 hours of being aware of the possible breach, you may need to raise an initial report with ICO, if you think it may be reportable. A reportable breach can have an interim report, but the important thing is to make sure that a) you are doing something about it, and b) that you have an audit trail on your discoveries and actions.

The ICO have further, clear guidance on this and it is worth making sure your Data Protection Lead in your school and your DPO is on top of this as well. If there has been more data taken and it poses a high risk to the rights and freedoms of data subjects (your staff, your children, your parents and any other individuals you may have personal data on), then there is a duty to also inform them. Be sure to read further advice from ICO on this.

The main thing about this is not to panic. Deal with things in a timely and methodical manner and use it as a chance to ensure that staff can deal with issues like this. As the NCSC say, there should be no blame culture with affected staff. Phishing scams get harder to spot every day, and even the best of us get caught out at times. It is also a good time to make sure that you are fully registered with the ICO, that you have stated who your DPO is and that your DPO's details are also on your Privacy Notice.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#ib1

GDPR
In Schools