Date: 3.11.26

Dear Parent/Carer

We are currently investigating a cyber-attack affecting the Trading with Schools (TwS) IT network, which provides internet and IT services to a number of schools and education settings across Bristol.

We have received information showing that during the attack on the network, documents and files were taken by the criminals behind these actions. Our investigators have now found evidence that these documents have been published online by the people responsible. This is called data theft. Put simply, it means information has been shared without permission.

We are now checking what information has been posted online, which schools may be affected and whether any information about pupils, families or staff is involved. We are still carrying out these checks and do not yet know the full impact.

When information is taken during a cyber-attack, there is a risk that it could be used to target people with scam emails, text messages or phone calls that appear genuine.

At this stage, we do not know whether information relating to your family has been affected. We are still finding out exactly what information may be involved. In the meantime, there are some simple steps you can take to help protect yourself and your family online.

How you can protect yourself

To help keep yourself and your family safe, we recommend the following:

- Be cautious of unexpected emails, text messages or phone calls, even if they appear to come from a trusted organisation. Criminals may use information from a data theft to make their messages look genuine.
- Do not click links or open attachments in messages you are not expecting. If you need to contact an organisation, use contact details from its official website rather than those included in a message.

Be particularly wary of messages asking you to:

- Reset your password;
- Verify account details;
- Provide personal or financial information;
- Claim compensation; or
- Take urgent action within a short timeframe.

Team/Service Area
Trading with Schools
Bristol City Council
Bristol

Website
www.bristol.gov.uk

Watch out for messages designed to create a sense of urgency or concern. Scammers often try to pressure people into acting quickly before they have had time to think.

If you receive a suspicious message that contains a password you currently use, change that password immediately. If you use the same password on other accounts, change it there too.

Use strong, unique passwords for important accounts such as email, banking and shopping websites. Where available, enable two-factor authentication for extra security.

Check your online accounts regularly for any unusual activity. This could include being unable to log in, changes to your security settings, messages you did not send or login attempts from unfamiliar locations.

Review bank and credit card statements carefully and contact your bank immediately if you notice any transactions or activity you do not recognise.

Reporting suspicious messages

If you receive a suspicious message:

- Forward suspicious emails to report@phishing.gov.uk.
- Forward suspicious text messages to 7726 (free of charge).
- If you receive a suspicious phone call, hang up and contact the organisation directly using trusted contact details.
- If someone claiming to be from your bank contacts you unexpectedly, end the call and contact your bank using the number on the back of your card, through your banking app, or by calling 159 to be connected safely to your bank.

Further updates

Our investigation is ongoing and we are continuing to assess the information that has been published. As we learn more about the impact of this incident, we will provide further updates and guidance to schools, staff, parents and carers. In the meantime, following the advice above can help reduce the risk of fraud, scams and unauthorised access to your online accounts.

Vik Verma
Director of Education and Skills
Bristol City Council, City Hall, BS1 5TR