View this email in your browser

www.onewest.co.uk

Important - Please pass to your Business Manager & share with staff

Avoiding COVID-19 Cyber Scams

Advice on avoiding COVID-19 Cyber Scams

Unfortunately some people are attempting to benefit from COVID-19 by **scamming** others.

ActionFraud has reported a 400% increase in reports of Coronavirus related fraud. These are mostly using the outbreak to lure people in to clicking links or opening attachments.

Some of the most recent scams to be wary of are:

- **Support for free school meals**

Parents have received **fake emails** stating *'As schools are closed, if you're entitled to free school meals, please send your bank details and we'll make sure you're supported.*' This is an attempt to steal money.

- **Change of payroll details**

Services managing payroll are receiving **bogus emails** saying *'Change of Direct Deposit Information'* apparently from employees. The email informs the employee has changed their bank account for pay deposits. It is thought that people are being targeted via their **LinkedIn profile**.

- **Phishing emails with malicious attachments**

People are receiving **emails** that have malicious Word documents or other attachments containing embedded computer viruses.

One email (and there are others!) pretends to originate from the **World Health Organisation** and invites the recipient to open an attachment for advice on safety measures to prevent the spread of COVID-19.

- **SMS Phishing**

Fake COVID-19 **websites** are being registered, with text messages appearing to be from the Government urging recipients to click on the link. The websites have been found to contain **Trojan software** that is designed to steal people's financial information.

- **Fake NHS donations**

ActionFraud has received many reports of a **scam email** purporting to be from HM Government, asking for **donations** to the NHS during the COVID-19 outbreak.

The bottom line is that if you weren't expecting the contact and if it doesn't look or feel right then it's probably not legitimate.

If you are still unsure then:

- **Hover (don't click!)** on the link - it will show you the address it's trying to take you to. Beware - The address may look genuine, but have some

slight spelling differences, or use of symbols/numbers to trick the brain into thinking it's reading something legitimate.

- **Consider** how you could **verify** the validity of what you have received. Can you ring the sender on a trusted line (e.g. obtained from an official website)?

If the worst happens and you click a link don't panic! – ensure you change your password and report it to your IT provider ASAP. If you would like further advice don't hesitate to drop us a line: One_West@bathnes.gov.uk

Our continued best wishes whilst the Lockdown continues.

Regards

The One West Team

Our mailing address is:

One_West@bathnes.gov.uk

Want to change how you receive these emails?

Drop us a line - we will be happy to help