www.onewest.co.uk

One West

Important information regarding a rise in cyber security incidents

Please pass to your Business Manager & Head of IT

Everyone wants to work without issues. These days though, we have no choice but to be very careful indeed with our IT. In particular, that means vigilance.

As a provider of specialist professional services including Cyber Security, we think it's important to ensure you know what might be coming your way.

Our Cyber Security team have released the information below which we strongly recommend you read.

If you have had it already apologies, we want to ensure as an important & urgent warning it reaches you!

To help if things escalate, we will be releasing additional information & guidelines over the next 6 weeks. We hope these will lend some support in managing future security.

Many thanks – I hope it is useful

Steve de-Bruin

Head of Client & Business Services

Cyber Security Precautionary Warning - Steady Rise in Number and Scope of Cyber Incidents

In recent days in the national press there has been increased reporting of cyber security incidents both here in the UK and in Europe. For example;

- European Banking Authority hit by Microsoft Exchange hack (Source - BBC News website, 8 Mar 2021)
- University of Central Lancashire among three hit by cyber-attacks (Source - BBC News website, 10 March 2021)
- Exchange email hack: Hundreds of UK firms compromised (Source - BBC News website, 12 March 2021)

In some instances, attacks have been part of state led campaigns and in other instances, they are likely to have been simple criminal activity.

Rather than focus just on high worth commercial targets, attackers seem to be now looking for new opportunities in both local government and the education sector.

We are aware of current investigations into major ransomware attacks in one council and one MAT.

This emphasises the importance of protecting both your educational and administrative networks.

In September, last year, the National Cyber Security Centre (NCSC) issued an alert to the academic sector following a spate of online attacks against UK schools, colleges and universities.

This is available on the NCSC website at the following link : https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector .

The recent increase in cyber activity might be timed to coincide with the return to schools when your attention is focused on dealing with the pandemic.

Trusts, academies and schools are urged to read the NCSC's newly-updated guidance on mitigating malware and ransomware attacks & to develop an incident response plan which they regularly test. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks .

Crucially, your technology team should be managing your connection to the internet, your networks and the devices connected to those network but it is important to remember the pivotal role of all of your staff and pupils in maintaining your organisations cyber security.

Quite often malware gets into networks by the inadvertent 'clicking' of what appears to be a safe link attached to an email.

Hence, regular notices about cyber related risks in school newsletters & regular training are invaluable reminders of the importance of cyber security.

It is never too early to start thinking of about it: this week the NCSC released guidance to Early Years practitioners about using cyber security to protect those learning environments also. It *can be read here: https://www.ncsc.gov.uk/news/early-years-providers-helped-to-take-first-steps-with-cyber-security*

Please keep safe while educating our future.

One West Cyber Security Team

Our mailing address is:
One_West@bathnes.gov.uk

Want to change how you receive these emails? Just let us know