November newsletter

WELCOME

Following on from our client survey work earlier this year, a number of our clients told us they'd like to hear from us more often. So, we have now introduced a monthly newsletter.

Like us, you may well be "GDPRd" out, with all the emails etc in the run up to May.

As part of our preparation we now have Cyber Essentials, Cyber Essentials+ and IASME accreditation.

Why do you need to know this?

Because it is a quality standard to reflect how seriously we take computer security and the protection of your data.

If you'd like to learn more about these accreditations for your business, please let us know.

Riven Support Agency app

if you don't already have this on your PCs we will be installing it shortly. This allows us to monitor and remotely control your machine, should you experience a problem.

For you, the good news is that you can use the

app to log support requests, and track where we are in fixing your problem.

Do give us a buzz on **01784 437 123**, if you have any concerns, or want to find out more.

We hope you enjoy reading the newsletter, and do let us know if you have any specific topics you'd like to learn more about.

Best wishes from
All of the team at Riven

HEADS UP!

We will use this space each month to flag any things we think you should know about:

Windows Server 2008 and **Windows 7** is close to end of life, and will no longer be supported by Microsoft from January 2020. If this affects you, be reassured that we will be in touch shortly to plan next steps.

Laptops and PCs – due to the increased need for power and memory with ever more sophisticated apps, we are now specifying a minimum of 8GB RAM, and Intel i5 core processor and solid state hard drive for all new machines.

You will notice significantly improved speeds and performance with the improved spec.

SECURITY FOCUS

As cyber security continues to be a core focus and concern for all of our clients, we will continue to share tips and key information to help you keep your data safe.

This month, we look at phishing. If you're not sure what that is, you may find this blog article a good start: https://www.rivenassociates.co.uk/gone-fishing-or-phishing.

One of the biggest security risks is often a company's own employees. It is wise to ensure your team have regular training, to keep them informed on security threats.

We have seen a significant increase in phishing threats with emails coming from a number of seemingly professional corporates including banks, Microsoft and even Government departments.

Do you think your team would be duped? Well, now you can tell for certain. We can set up a

portal, using Sophos software, which will send spoof phishing emails purporting to be from organisations like Amazon, Office 365 or the Post Office to see if your staff would be fooled into providing login details or clicking on links.

You can login at any time to see which staff failed the test. We recommend anybody who failed takes a short online training session, highlighting the risks, to ensure they don't get duped by a real phishing attempt in the future.

If you'd like to know more about running this in your business, please contact us on 01784 437 123.