Technology Insider

YOUR MONTHLY NEWSLETTER, WRITTEN FOR HUMANS NOT GEEKS

Bluegrass® Computer Services a Modern Networks company

JUNE 2023

Bluegrass® TechnologySupportInnovation

modernnetworks

Bluegrass joins forces with Modern Networks

Modern Networks joins forces with Bluegrass to extend its presence in the South West.
Bluegrass is pleased to announce that the company has joined forces with Modern Networks. The investment is part of Modern Networks' long-term strategy to grow its business via both organic and inorganic growth following investment by Horizon Capital in April 2021.

We've have been talking to Modern Networks for a year now and how Bluegrass will sit as part of their excellent service offering, and we have to say we're really excited by the opportunity.

Better together
The merger of Bluegrass and Modern Networks will result in a more robust and competitive company. This partnership will provide Modern Networks with additional regional coverage, and enhance our position in the commercial property sector in the Southwest.

For all intents and purposes, it will be business as usual. Chris will be staying along with the excellent team of engineers and sales. Dave will be staying on in a part-time consultancy roll for six months and then both Dave and Hilary will start their deserved retirement.

Accelerated growth
With this union, we aim to create a larger, more diversified business that can better cater to our customer's needs and expand into new markets. Through the merger, we will also be able to provide our customers with improved customer support, thanks to a larger team of skilled IT professionals and a more reliable service infrastructure.

Our ultimate goal is to build a stronger, more competitive company that can provide unparalleled service to our valued customers.

No changes for now
Initially, Bluegrass and Modern Networks will continue to trade under their existing brand names. However, over time Bluegrass will be integrated into Modern Networks.

Bluegrass customers can rest assured that the excellent services and support they enjoy today will remain unchanged and Modern Networks are equally committed to providing excellent customer service. Of course, we will be writing to each customer personally with more detailed information.

Committed to our customers
Bluegrass and Modern Networks have a track record of working closely and developing in-depth, long-term customer relationships. As a united business, we remain committed to our customers and providing innovative IT, telecommunications and broadband services that meet your specific needs.

Matt Reeve, CEO of Modern Networks said "Joining forces with Bluegrass grants Modern Networks a valuable foothold in the South West, bolstering our regional presence. Our goal is to enable business growth in this area, aspiring to become the preferred IT service provider in the region."

To learn more about Modern Networks acquisition of Bluegrass, please visit www.modern-networks.co.uk/news

It's an exciting time for Bluegrass, the next chapter begins. If you have any queries about this update please give us a call on 01392 207194 and we'll happily help.

All the best

Chris, Hilary and Dave

Is it time to ditch pass-words for passkeys?

Passwords are the most used method of authentication, but they are also one of the weakest. Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This makes them vulnerable to cyber-attacks.

The sheer volume of passwords that people need to remember is large.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

Advantages of Using Passkeys Instead of Passwords

More Secure

One advantage of passkeys is that they are more secure than passwords. Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location.

This makes it much harder for hackers to gain access to your accounts.

More Secure

Another advantage of passkeys over passwords is that they are more convenient. With password authentication, users often must remember many complex passwords.

This can be difficult and time-consuming. Forgetting passwords is common and doing a reset can slow an employee down.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts. It also reduces the likelihood of forgetting or misplacing your password.

Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need thedevice passkey authentication to breach the account.

NEW TO Microsoft 365

Printing gets a security boost

Microsoft 365 is helping to reduce print waste and increase privacy with an update to its printing function.

It will hold print jobs until you arrive at the printer. Then you scan a QR code on the Microsoft Office mobile app to start your print job. Clever, right?

It's called Secure Release Printing, and you can ask your IT partner to get it set up for you.

TECH UPDATE

Are you asking ChatGPT the wrong questions?

ChatGPT is incredible, but it still has its limitations. If you find it frustrating and inaccurate, it's quite likely you're doing it wrong. Here's how to get the best out of it...

Be specific: A basic question will generate a basic answer. The more specific your question, the more likely it is to create a good answer.

Give it context: For instance, if you're asking it to review an email, tell it whose perspective it's reading it from – an employee, a frustrated client, and so on.

This is how you can get in touch with us:

CALL: 01392 796779 | **EMAIL** ask@bluegrass-group.com
WEBSITE: www.bluegrass-group.com

Bluegrass® Computer Services
a Modern Networks company

Is your business missing *a cyber resiliency plan?*

A recent cyber security report found that just 11% of IT budgets go into incident response, disaster recovery, and infrastructure security.

This could be a dangerous underinvestment.

While it's vital to keep your data and infrastructure protected with a layered, multi-stranded approach, no network can ever be protected from 100% of attacks. Even if it were possible, it would make your systems hard to live with, and would certainly destroy productivity.

That means you need a cyber resiliency plan to help you respond to any cyber attack that does get past your defences. It requires different thinking to your other resilience plans around physical disasters.

In the case of a flood for example, your incident response might be to get cleaned up, find a temporary work location and get your systems online again. But in the case of a ransomware attack, you'd need to investigate how the attack occurred, locate and patch the holes in your defences, and remove all traces of the attack from your systems.

For a cyber attack, you'll also have a different RTO – a Recovery Time Objective – which defines how quickly you expect to get back up and running. Your resiliency plan should define that RTO, so that you understand what downtime costs you'll be facing.

Where do you start? We recommend:

1. **Improving your security:** Hopefully you've already ticked this one off. Make it as hard as possible for crooks to access your systems, without creating measures that are so hard to live with that they interfere with the smooth running of your business.
2. **Monitoring your systems:** The sooner you detect an attack, the faster you can respond, which will minimise any damage. You should always be monitoring for suspicious activity and staff should be trained to spot warning signs.
3. **Responding swiftly:** Your response plan should be available to everyone in the business, and should include information on who to report a suspected breach to, and all the steps that should be taken.
4. **Making recovery easier:** Once an attack is under control it's time to recover. That means having a good backup in place, and a rehearsed plan for restoring your systems.

If you need help with cyber resiliency, or other disaster recovery plans, get in touch today.

Tech Fact!

One of iTunes' terms and conditions states that you are not to use their devices to create "...nuclear, missile, chemical or biological weapons"

DID YOU KNOW?

Snipping Tool lets you record your desktop?

The updated snipping tool in Windows 11 allows you to record your desktop – it's a great way to produce training videos for remote workers (or anyone else, for that matter).

You can choose which section of the screen you record, with videos saved in MP4 format.

This is how you can get in touch with us:
CALL: 01392 796779 | **EMAIL** ask@bluegrass-group.com
WEBSITE: www.bluegrass-group.com

Bluegrass® Computer Services
a Modern Networks company

Monthly update from Dave

Being totally honest with you, when I first founded Bluegrass back in 2007 I didn't have a vision on what the business would become.

Our goal was to deliver a high quality service that had the user at the centre benefiting from good communication and an understanding that we felt their pain when something went wrong. I believe that despite changes with technology and ways of working that we have maintained that value.

No matter what values or goals a business has, the strength of a business comes from the people in the business. We're very fortunate to have a wonderful team who have embraced our goal and one that stands firm after 16 years.

Over those 16 years I've been so lucky to not only work with great people but to have supported many incredible businesses.

However, there comes a point when it's time to hang up the boots (football reference!) so that we can spend time with our children and their children.

Eighteen months ago Chris, Hilary and I started the process of looking for another company who had the same values as we did, that could take Bluegrass forward. We eventually came across Modern Networks in April 2022.

Since then we've got to know Matt Reeve (CEO) and his team, and during that time they've demonstrated a passion for providing a high quality of service with happy employees. We're extremely happy to pass the Bluegrass baton to Matt with the knowledge that the new Bluegrass will go from strength to strength.

The Bluegrass team are ready and waiting to help you.

I wish you all the best for you and your business.

Regards

Dave

Not delighted with your IT Support?

We'd love to chat.

We offer flexible IT support packages that can be tailored to your business.

We support in house teams or can be your complete IT Partner.

Request a quote today.

Question: My employees use WhatsApp to share work info – should I stop this?

Answer: If you're already using a communication tool like Teams, your people should keep all work communication there. It's more secure and can save a lot of time hunting for information. WhatsApp is not an app that you should be using in your business for sharing work information.

Question: I've heard I can upgrade to Windows 11 without TPM 2.0?

Answer: A TPM is a tiny security chip on your machine which is required by Windows 11. There is a workaround, but our advice is to avoid it. It may mean you miss out on key security updates, which could leave your entire network vulnerable.

Question: I've lost my laptop. What do I do?

Answer: You should have a response plan in place for this type of incident. Report it to the correct person so that data can be wiped remotely to avoid a breach. If you don't have a plan or remote management in place, we can help.

This is how you can get in touch with us:

CALL: 01392 796779 | **EMAIL** ask@bluegrass-group.com
WEBSITE: www.bluegrass-group.com

Bluegrass® Computer Services
a Modern Networks company