Technology Insider

YOUR MONTHLY NEWSLETTER, WRITTEN FOR HUMANS NOT GEEKS

Allign your team to company targets with Microsoft Viva Goals

You often hear the words "digital transformation" and collaboration." But what do they actually mean? What do they mean for the day-to-day of running your business?

Collaboration can't happen without shared goals. When departments are siloed and unconnected, priorities can conflict. People are doing their best but may not be moving in the same direction.

Digital transformation is simply the use of technology to better reach business goals. This encompasses moving from analog ways of doing things. Transitioning to tools that are more automated and connected.

Microsoft has been at the forefront of digital transformation and collaboration. Its Viva platform drives an improved employee experience. It does this by use of AI, automation, cloud connectivity, and more.

What is Viva Goals?

Viva Goals is one of the newest Viva applications from Microsoft. It connects teams so they're moving toward a shared set of goals. Employees align, whether someone works in the accounting department or customer support.

Business leaders can look at Viva Goals as a way to solidify company objectives. They can then tie these objectives to meaningful targets for each department.

For example, say you have a corporate target to provide exceptional customer support. This goal by itself is generic. It doesn't connect to what teams need to do to make it happen.

In Viva Goals, that target can have directives for various teams. Such as customer support reducing ticket resolution by 8 hours. This brings goals to a meaningful level and allows organisations to track progress.

Here are the key value-adds of using Viva Goals.

- Aligns your team to the same goals
- Maintains focus on your goals
- Integration with Teams and Microsoft 365

The integration with Teams keeps goals front and center. Employees get recognised for meeting targets and helping the company achieve its goals.

This keeps everyone engaged and moving together.

Overcoming barries for BYOD

Mobile devices make up about 60% of the endpoints in a company network. They also handle about 80% of the workload.

But they're often neglected when it comes to strong cybersecurity measures. This is especially true with employee owned mobile devices.

Purchasing phones and wireless plans for staff is often out of reach financially. It can also be a pain for employees to carry around two different devices.

This has made BYOD the preferred way to go by about 83% of companies. Here are some tips to overcome the security and challenges of BYOD.

Define your BYOD Policy
If there are no defined rules for BYOD, then you can't expect the process to be secure.

Employees may leave business data unprotected. Or they may connect to public Wi-Fi and then enter their business email password, exposing it. If you allow employees to access business data from personal devices, you need a policy. This policy protects the company from unnecessary risk.

Keep your Policy "Evergreen"
As soon as a policy gets outdated, it becomes less relevant to employees. Thus, they may tend to ignore it. Make sure to update your BYOD policy regularly.

Use VoIP apps for business calls
Customers having employees' personal numbers is a problem for everyone. Employees may leave the company, and no longer answer those calls. The customer may not realise why.

You can avoid the issue by using a business VoIP phone system. These services have mobile apps that employees can use. VoIP mobile apps allow employees to make and receive calls through a business number.

Create restrictions on saved company Data
No matter what the type of device, you should maintain control of business data.

It's a good idea to restrict the types of data that staff can store on personal devices. You should also ensure that it's backed up from those devices.

Require device updates
When employee devices are not updated or patched, they invite a data breach. Any endpoint connected to your network can enable a breach. This includes those owned by employees.

An endpoint device manager can push through automated updates. It also allows you to protect business data without intruding on employee privacy.

Include BYOD in your offboarding process
If an employee leaves your company, you need to clean their digital trail. Is the employee still receiving work email on their phone?

Do they have access to company data? Are any saved company passwords on their device?

Make sure you check all this during offboarding.

NEW TO Microsoft 365

OUTLOOK
Outlook's bringing better notifications to mobile

This month we're expecting to see a change to the way Outlook notifications work on mobile, starting with Android.

Microsoft is making it easier for you to customise your notification settings, so you can stay on top of things without sacrificing your work/life balance.

WORD
Assign tasks from within Word

Teams is a great tool for creating and assigning tasks to people, but have you ever thought it would be good to do it directly within the document you're working on?

Microsoft will allow you to create, assign and track tasks within your Word document – simply by using @mentions.

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

Bluegrass®
TechnologySupportInnovation

Does it really matter what Browser you use?

YES!

The web browser you choose can have a big impact on your online security. And as a business, it's important you don't take any unnecessary risks, even if you're someone who likes to steer clear of the IT megabrands.

As well as allowing advertisers to track your online activity, there are often bugs and vulnerabilities in lesser-known browsers that cyber criminals can exploit to not only steal your data, but to compromise your entire network.

And while it's vital that you choose your browser carefully (and stick to the same browser across the business), it's equally important to make sure you run updates and patches as soon as they become available to keep your browsing as secure as possible.

You may already know that Google's Chrome is the most popular desktop browser in the world – more than 6 in 10 people use it. It's fast, easy to use, and it has built-in phishing and malware protection (though you shouldn't rely solely on that).

Next comes Apple's Safari, followed by Microsoft Edge.

Edge is similar to Chrome in that it's fast, customisable and simple to use. It also gives you clear privacy options, which are super-important when using a browser for business. As a Microsoft product, it's the default browser for Windows 11, and comes with some Microsoft-specific links. So if you use Windows 11 and haven't tried Edge, give it a go.

The key thing to keep in mind when choosing your browser is security. Don't just stick with the standard settings – customise them to suit your business. Look at the threats you may face, the settings that can help protect against them, and the usability… all in equal measure.

It seems like a relatively simple task to choose a web browser, but there's more to it than you think if you want to take security seriously (and you should!)

Can we help recommend the best browser for your business? Or make sure you're getting the most from your current browser's security settings? Get in touch, we're here to help.

DID YOU KNOW?

If you use Google Chrome as your browser, did you know there's a way you can check exactly how secure it is at any time?

Go to the browser's Settings, and select Privacy and Security. On the right, under Safety check, select Check now.

This checks for updates, looks at the strength of your stored passwords and tells you if browsing is safe and if you've downloaded a harmful Chrome extension.

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

Bluegrass®
TechnologySupportInnovation

Monthly update from Dave

Have you scheduled any employee cybersecurity awareness training yet for 2023? It's often something that gets put on the back burner after things like revenue initiatives and software up-grades. Yet, human error is a big driver of cyberattacks.

People don't usually click on phishing links because they want to. They don't purposely make their accounts easy to breach. Many don't know any better. Others know better, but rarely hear management talking about cybersecurity, so they don't feel it's a priority.

One fact that may surprise you is your reduction in risk with well-trained employees. When teams are regularly taught security awareness it can reduce cyber risk by as much as 70%. That's a big difference!

Think about that when looking for ways to improve your bottom line this year.

Reducing risk reduces the chance you'll get hit with a costly cyberattack. Train employees regularly and you can reap tangible benefits while building a culture of cybersecurity.

If you need help putting together engaging security awareness training, just let us know.

Get in touch, we can help.

Regards

Dave

Joint Managing Director

Q & A

Question: What's Focus Assist in Windows 11?

Answer: Focus Assist takes Do Not Disturb a step further. It can hide distracting icons from your Taskbar and give some notifications more priority than others. Use it together with Do Not Disturb and you'll be able to block out distractions to better focus on work.

Question: Can I share a Word document without someone changing it?

Answer: Yes! Just click the editing button next to the share button in the top right of your screen. Then simply select whether you'd like people to be able to edit, view, or review the document. You can switch it back whenever you're ready.

Question: My files keep opening in the wrong application. Help!

Answer: This is a frustrating problem, but an easy fix. Right click the file you want to open and select 'Open with' then 'Choose another app'. Then check the box that says 'Always open with this app'.

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.

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

Bluegrass®
TechnologySupportInnovation