Technology Insider

YOUR MONTHLY NEWSLETTER, WRITTEN FOR HUMANS NOT GEEKS

Bluegrass®
TechnologySupportInnovation

August 2022

Are you blacklisting or whitelisting?

You know what it means to be blacklisted, right? (we don't mean through personal experience, of course).

Blacklisting is where you block something you don't trust. It's used to keep networks and devices safe from bad software and cyber criminals.

But there's another, safer way of doing that – and that's called whitelisting.
Rather than trying to spot and block threats, you assume everyone and everything is a threat, unless they've been whitelisted.

But which is the right approach when it comes to keeping your business data safe? This debate rages on, with many IT professionals holding different views.

Here are the main differences…

- Blacklisting blocks access to suspicious or malicious entities
- Whitelisting allows access only to approved entities
- Blacklisting's default is to allow access
- Whitelisting's default is to block access
- Blacklisting is threatcentric
- Whitelisting is trust-centric

There are pros and cons to each approach.

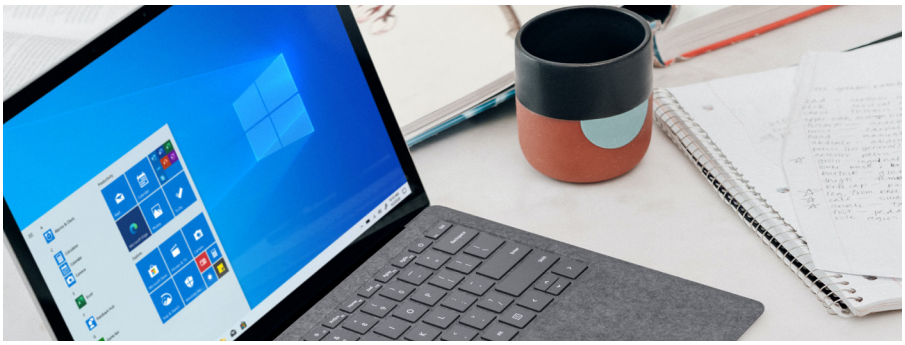
Whilst blacklisting is a simple, low maintenance approach, it will never be comprehensive as new threats emerge daily. It's also easy to miss a threat, as cyber criminals design software to evade blacklist tools.

Whitelisting takes a stricter approach and therefore comes with a lower risk of access.

But it's more complex to implement and needs more input. It's also more restrictive for people using the network and devices.

Confused? You're not alone!

If you'd like to discuss which approach is best for your business, get in touch.



5 ways Microsoft can support a hybrid office

Offering a hybrid office has become critical to attracting and retaining staff, but how do you ensure your productivity levels remain high?

Technology is the ky enabler of this, specifically Microsoft 365.

Here's 5 new features that can help:

RSVP in Outlook
Everyone knows the benefits of operating a hybrid office, but sometimes it can be tricky to keep track of which colleagues are in the office on which days. When you book a meeting, it's hard to know if they'll be joining face to face or virtually. Well Microsoft have added a feature that will allow users to RSVP to meetings letting team members know how they'll be attending, in person or virtually.

Front Row feature in Teams
Online meetings can be hard work. Especially when you have lots of people on a call and you can hardly see their faces on the screen. Microsoft have launched a new feature called Front Row into Teams and it brings the video gallery of faces to eye level at the bottom of the screen. This encourages more interaction with the people in the meeting as their face is more visible and in a more natural position.

Cameo in PowerPoint
Microsoft have recognised that the use of PowerPoint within teams can be a bit clunky. So they're improving the integration of the two tools. You can now use a mode to access your presenter notes without having the audience see them, but they're also adding a new feature called Cameo. Cameo allows you embed your camera feed straight inside any of your slides for a more immersive audience experience.

Mesh in Teams
Not yet released but coming later in the year, Mesh for Teams is going to bring the virtual world to life in your online meetings. You will be able to create 3D avatars that look just like you, for times when you don't want to have your camera on. They will also enable full 3D environments where you and other avatar colleagues can collaborate online in a whole new experience. Watch this space.

Microsoft Loop
Again a feature not quite yet fully released is Microsoft Loop, possibly a bit of a rework of Microsoft Fluid which was designed for real time collaboration. Loop will enable users to add a collaboration interface to any of the products within the Microsoft suite. Loop will be made up of three main offerings; Components, Pages (also referred to as canvasses) and Workspaces.

New in Microsoft 365

Hit send too soon in Outlook?

We've all accidentally sent an email before it was ready. Or sent it to the wrong person.

And while Outlook's recall is a popular feature, historically it hasn't always worked.

It was only reliable if the recipient used Outlook too.

Great news.

An update due for release next month will make email recall work regardless of where the recipient gets their email.

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

Is MFA really secure?

Data breaches are on the rise and now with most businesses storing their data in the cloud, a users password is the quickest way for a hacker to get in and do some damage.

Added Multi-factor authentication (MFA) is one of the best ways you can protect your business.

MFA adds an extra layer to your sign in process. It requires an extra step to be taken before you're allowed in. This extra step is time sensitive too.

There are three methods for MFA:

SMS Based MFA

Firstly when you set up this type of MFA, you need to provide a mobile number where you're happy for the codes to be sent. Then when you attempt to log in to the particular application, the system automatically sends you a random time sensitive code to your mobile phone. Only once this code has been input correctly do you gain successful access. It's safe in that you need both username, password and access to your mobile phone in order to log in to a cloud based app.
So unless someone knows your credentials AND has stolen your mobile phone, then it's a pretty safe bet.

On-Device App MFA

Pretty similar to the SMS based MFA, however instead of receiving a text message with the code, you open up an authentication app in your phone. This provides you with a time sensitive code instead. Apps that can do this include Authy, Authenticator, 2FA Authenticator and many more. Microsoft and Google of course have their own version too.

Security Key

This method again uses a random code, but it is automatically entered by the insertion of a special security key into your PC or mobile device. You purchase the key when you initially set up the MFA solution. This is a safe method as again, only you have the key, but of course you then have to carry it everywhere you go and not lose it!

It must be noted that SMS is now the least secure method of the three because malware exists that can clone a SIM card, allowing hackers to receive those text messages too.

If you have highly sensitive data we'd always recommend the security key method, but if not go for the On-device app option.

Want some help setting this up, call us today on 01392 796 779.

Tech Fact!

In the 1950s, computers were called 'Electronic Brains'. Shall we stick with 'computer'?

DID YOU KNOW?

paying ransomware makes you a bigger target?

Ransomware is evil. It's where your data is encrypted until you pay a ransom fee to get it back. Many business owners say they'd pay the fee to resolve the problem quickly. But doing that can make your business an even bigger target for attacks.
80% of ransomware victims who paid up were then hit a second time by the same attackers.

Doh.

The greatest defence against ransomware is being 100% prepared. You need a working and verified backup, a ransomware resilience plan, and all the right security measures in place **BEFORE** you are attacked.

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

Do you remember the days before text messages? It's hard to imagine them now. SMS has become a normal part of our life.

We text customers, friends, family, and work colleagues just about daily. It's quicker than email and you get to use a bunch of cool emojis!

For the most part, people have been able to count on the fact that only those people or businesses that they gave their mobile number to will show up in their text messages. But this is, unfortunately, changing rapidly. Mobile numbers are no longer private. Scammers can get them from the Dark Web and unscrupulous marketers who will sell cell phone lists to anyone.

SMS is fertile ground for phishing scams. First, people are not yet expecting to get fake texts, second, it's much harder to tell who the sender is with no email address. How bad has phishing by SMS (known as smishing) gotten? It skyrocketed nearly 700% in just the first 6 months of 2021.
If your company doesn't have training in place to warn employees about SMS phishing scams, their devices could easily set off a full network breach. We recommend getting a mobile device management solution that can secure those smartphones.

Speak to us today about training if you think you need some help.

Regards

Dave

Joint Managing Director

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

How can I avoid being phished?

Answer

The best thing is treating every email with caution. If you're unsure, check the address it's been sent from, look for grammatical errors, and see if the layout looks like a normal email from that person or company. If you're unsure, don't click any link.

Question

What's an insider threat?

Answer

It's the name for when someone within your business gives cyber criminals access to your devices or network. Usually it's not malicious. But it's why regularly training your team in cyber security is a must.

Question

How do I choose the right backup for my data?

Answer

Security and reliability should be your main considerations. Get in touch and we'll tell you what we recommend.

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