Technology Insider

YOUR MONTHLY NEWSLETTER, WRITTEN FOR HUMANS NOT GEEKS

Bluegrass®
TechnologySupportInnovation

October 2022

# Do you know exactly what services your staff are signing up for?

**Whatever problem, need or want you have… there's a cloud application out there that can help you.**

We've never lived in a such a rich time for problem solving. Every day, hundreds of new services launch to make our lives easier and help us be more productive.

These applications all live in the cloud. They're known as Software as a Service (SaaS) because you don't load any software onto your device. You use them in your browser.

We would argue this SaaS revolution over the last 15 to 20 years has played a critical part in shaping the way we work today.

However, there's an issue. Many businesses aren't 100% aware what new services their staff have signed up to. And this problem isn't a financial one, it's a security one.

Let's give you a scenario. Suppose a member of your team, Sharon, is trying to do something creative, but just can't with her existing software. She Googles it, and finds a cool application.
Sharon signs up for an account, and as she's in a rush uses the same email address and password as her Microsoft 365 account. Yes, reusing passwords is very bad practice and common. But this gets worse.

She uses the application for half an hour to achieve what she needs to do… and then forgets it. She's got no intention of upgrading to a premium subscription, so just abandons her account.

That's not an issue… until 1 year later. When that SaaS application is hacked by cyber criminals, and all of its login credentials are stolen.

It's well-known that cyber criminals will try stolen details in other sites, especially big wins like Microsoft 365.

Can you see the issue here? Sharon's 365 account would be compromised and she'd have no idea how it happened. She won't remember an app she used for half an hour a year ago.

The answer is to have a solid policy in place about who can sign up for what kind of service. Also ask your technology partner if they have any way to track what apps are being used across your business.

And definitely get a password manager for your staff… this will generate a new long, random password for each application, remember it and **autofill login boxes.**

Password managers encourage good password practice because they make it easy.

# Technology update

## SMALL BUSINESSES ARE ATTACKED BY HACKERS 3X MORE THAN LARGER ONES

Have you felt more secure from cyberattacks because you have a smaller business? Maybe you thought that you couldn't possibly have anything that a hacker could want? Didn't think they even knew about your small business.

Well, a new report out by cyber-security firm Barracuda Networks debunks this myth. Their report analyzed millions of emails across thousands of organizations. It found that small companies have a lot to worry about when it comes to their IT security.

Barracuda Networks found something alarming. Employees at small companies saw 350% more social engineering attacks than those at larger ones. It defines a small company as one with less than 100 employees. This puts small businesses at a higher risk of falling victim to a cyber-attack.

### Small Companies Tend to Spend Less on Cybersecurity

When you're running a small business, it's often a juggling act of where to prioritize your cash. You may know cybersecurity is important, but it may not be at the top of your list. So, at the end of the month, cash runs out, and it's moved to the "next month" wish list of expenditures.

Small business leaders often don't spend as much as they should on their IT security. They may buy an antivirus program and think that's enough to cover them. But with the expansion of technology to the cloud, that's just one small layer. You need several more for adequate security.

### Every Business Has "Hack-Worthy" Resources

Every business, even a 1-person shop, has data that's worth scoring for a hacker. Credit card numbers, SSNs, tax ID numbers, and email addresses are all valuable. Cyber-criminals can sell these on the Dark Web. From there, other criminals use them for identity theft.

### Small Businesses Can Provide Entry Into Larger Ones

If a hacker can breach the network of a small business, they can often make a larger score. Many smaller companies provide services to larger companies including digital marketing, website management, accounting, and more.

### Small Business Owners Are Often Unprepared for Ransomware

Ransomware has been one of the fastest-growing cyberattacks of the last decade. So far in 2022, over 71% of surveyed organizations experienced ransomware attacks. The percentage of victims that pay the ransom to attackers has also been increasing. Now, an average of 63% of companies pay the attacker money in hopes of getting a key to decrypt the ransomware.

## Helpful Microsoft feature

### SAVE RECURRING EMAIL TEXT IN OUTLOOK'S QUICK PARTS

Do you have certain emails you send to customers that have the same paragraphs of text in them?

For example, it might be directions to your building or how to contact support.

Stop retyping the same info every time.

Outlook has a feature called Quick Parts that saves and then inserts blocks of text into emails. Create a Quick Part by high-lighting the text to save in an email.

- On the Insert Menu, click Quick Parts.
- Save Quick Part.
- When ready to insert that text into another email, just use the same menu.

Then click to insert the Quick Part.

## 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

# Would you pay if YOUR business was crippled by ransomware?

**Ransomware is scary. It's where cyber criminals lock your data and charge you a ransom fee to get it back.**

If it happened to you, would you pay the fee?

Despite what the criminals promise, they don't always unlock data when the ransom fee is paid. Or they ask for a second fee. Or they unlock it and then sell it on the dark web anyway.

Many large companies are now refusing to pay, finding other ways to get their data back. And ransomware groups are looking for different opportunities.

Small, financially stable businesses are the new targets. And the size of payments demanded has increased.

This means you and your team need to be vigilant about cyber security. Continue to take the necessary precautions such as using a password manager, checking emails are from who they say they're from, and making sure your network is being monitored and protected.

It's also vital that you have a working backup of all data. Check it regularly.

Even without paying the ransom demand, your business stands to lose a lot of money if hit by ransomware. It takes ages and can cost a ton to get back on your feet

If you want us to audit your business and check its ransomware resilience, get in touch.

## Tech Fact!

On average, there are 500,000 new internet users every day.

## DID YOU KNOW?

### Internet Explorer has lost all support

After being the main entry to the internet in the late 1990s and early 2000s, Internet Explorer (IE) is gone.

As of June 15, 2022, Microsoft dropped the web browser from support. To ease the transition away from Internet Explorer, Microsoft added IE Mode to Edge. This mode makes it possible for organizations to still use legacy sites that may have worked best in IE.

If you haven't yet addressed old copies of IE on your computers, your network could be at risk due to vulnerabilities in the browser no longer being fixed. Here's what you should do:

1. Migrate Browser Data to Microsoft Edge from IE
2. Uninstall the IE Browser
3. Ensure Employees Know How to Use IE Mode in Edge
4. Train Employees on Microsoft Edge Features

## 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

This is something I've spoken about before but it's so important that I'm covering the topic again and I make no apology for highlighting it.

The majority of SMEs believe that they don't need to worry about ransomware or phishing. That's like saying I don't have to lock my car and I can leave my front door open because no one will take advantage of me!

The chances are that someone in your business will receive at least one phishing email every week and if you don't have the right software tools or processes in place you'll get one ransomware email a month. This is a real problem. It will only take one person to innocently click on a link in an email or respond to a phishing email and the business could be in trouble.

I remember a conversation I had about the importance of cyber protection only to be told that "we're ok as we have antivirus and you support us". Antivirus is a very small but important form of protection that needs other solutions around it and IT support companies can only work within the confines of what the customer is prepared to accept and implement.

I accept that it's not possible to have 100% protection from such attacks but the more layers of protection you have the greater the chance that the cyber criminal will stop trying to compromise your business.

There are a multitude of solutions ranging from software to user education that will help safeguard your business. Some may cost but what would be the financial impact from the damage to your reputation, loss of customers, potential fines etc. if your business suffered from an attack. It's worth looking at both sides of the costs so that you can make an informed decision on the risk to your business.

Get in touch, we can 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

Should I let my team have work apps on their personal phones?

### Answer

It's personal preference. But if you do, make sure their phones are protected by the same security measures they'd have on work devices.

### Question

I've received an email that looks genuine, but hasn't addressed me by name. Should I click the link?

### Answer

If you ever have cause for doubt, don't click links or download files. Phone the sender to check if they really sent the email. It may take a few minutes but it's worth it.

### Question

Should I be monitoring my remote staff?

### Answer

Software exists to do this, but what message does it send to your team? It can be highly counterproductive in many cases. Take the time for regular catch-ups over Teams instead, or try a productivity tracker if you have concerns.

## 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