Technology
Insider

YOUR MONTHLY NEWSLETTER, WRITTEN FOR HUMANS NOT GEEKS

Bluegrass®
TechnologySupportInnovation

June 2022

Your remote workers aren't using devices like this are they???

When did you last check everything was OK with the devices your team are using when they work remotely?

That might sound like a strange question. But we recently discovered that 67% of remote workers are using faulty devices to work from. And the reason?

They've likely damaged the device themselves and are too scared to tell you! Laptops, keyboards and monitors are most likely to be damaged (in that order). And it's usually because of food or drink spills… though some people blame their partners, children, and even their pets! We've all watched in horror as a cat rubs itself against a full glass of water next to a laptop...

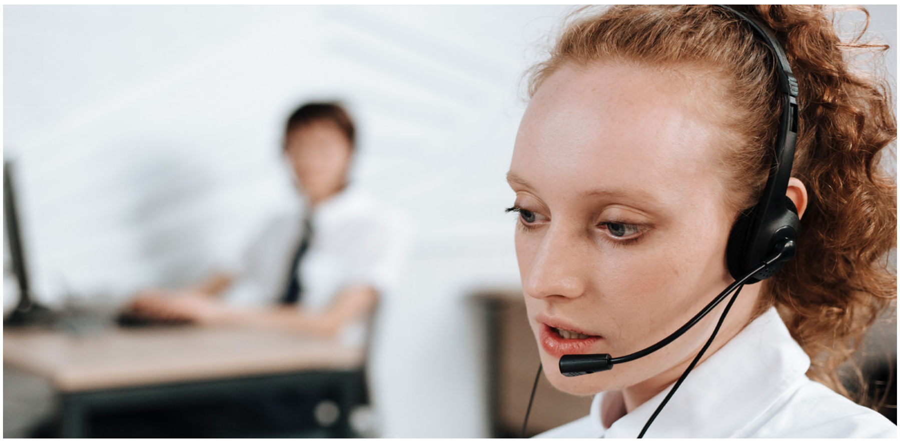
Using a device that doesn't work properly is a problem, of course.
First, it's going to damage your team's productivity. Tasks might take longer or be more difficult to complete.
If they try
to fix the problem themselves, they risk causing further damage.
No... a fork isn't a clever way to prise bits of cake out of your keyboard...

But the other issue is that of security. In some cases, your people will stop using their damaged company-issued device, and use a personal device instead. Which puts your data at risk. Because their personal devices won't have the same level of protection as your business devices.

It also means that if they're connecting to your network, it might not be a safe connection, potentially leaving the door open for cyber criminals.
And because your IT partner isn't monitoring personal devices, it's possible they won't spot an intrusion until it's too late.

Our advice? Make it a regular routine to check that everyone's happy with their devices. And have a policy that they won't get in trouble for accidental damage, so long as it's reported immediately.

If you need help replacing any damaged devices, just give us a call.



BOOST YOUR VOIP SECURITY

Given the variety of threats imposed by attackers on VoIP systems, it's necessary to optimize your VoIP security ASAP.

Here are 6 valuable tips to get you started.

Tip #1. Set Up a Firewall
If spam or a threat comes your way, the firewall will identify and gain control over it, shielding your system shielded from the attack. A good set-up will allow the data packets you send to travel unhindered.

Tip #2. Use Strong Passwords
Use randomly generated passwords consisting of at least 12 characters including numbers, upper- and lower-case letters and symbols. Most VoIP phones come with pre-set passwords, often available publicly, change these immediately.

Tip #3. Restrict Calling
Many VoIP attacks happen due to toll fraud. So, if your business runs locally, there's no need to have the international call option enabled. You should also block 1-900 numbers to avoid toll fraud.

Tip #4. Encourage Your Team to Report Suspicious Behavior
You should hold periodical Cybersecurity Training to keep your environment safe at all times. Train your employees how to spot unusual network activity and report suspicious behavior.

Tip #5. Deactivate Web Interface Use
Unless it's absolutely necessary for you to use the web interface, be sure to secure it very strictly. It's enough for a single phone user falling prey to leave the whole system exposed to an external party. All your data can be stolen in text format as a result.

Tip #6. Use a VPN for Remote Workers
Virtual Private Networks (VPNs) are great software that encrypts traffic regardless of your employee's location. You can set up such a network for your remote staff to prevent data leaks and breaches. A well configured VPN won't degrade the call quality.

Not yet made the move to VoIP? Call our team today to find out about our cost effective VoIP solutions.

New in Windows 11

If you've made the switch to Windows 11, you'll soon have a new power:

The ability to organise your Start menu apps into folders.

It'll work by simply dragging and dropping icons on top of each other to create folders.

You'll get this new power in an update in the next few months.

Top Cyber Security mistakes you might be making

The global damage of cybercrime has risen to an average of $11 million USD per minute, which is a cost of $190,000 each second. 60% of small and mid-sized companies that have a data breach end up closing their doors within six months because they can't afford the costs.

The costs of falling victim to a cyberattack can include loss of business, downtime/productivity losses, reparation costs for customers that have had data stolen, and more.

Here are the most common missteps when it comes to basic IT security best practices.

Not Implementing Muti-Factor Authentication (MFA)

Credential theft has become the top cause of data breaches around the world, according to IBM Security. MFA reduces fraudulent sign-in attempts by a staggering 99.9%.
it even easier for phishing via SMS to fake being a shipment notice and get a user to click on a shortened URL.

Ignoring the Use of Shadow IT

Shadow IT is the use of cloud applications by employees for business data that haven't been approved and may not even be known about by a company.

Shadow IT use leaves companies at risk for several reasons:

- Data may be used in a non-secure application
- Data isn't included in company backup
strategies
- If the employee leaves, the data could be lost
- The app being used might not meet company compliance requirements

It's important to have cloud use policies in place that spell out for employees the applications that can and cannot be used for work.

Thinking You're Fine With Only an Antivirus

No matter how small your business is, a simple antivirus application is not enough to keep you protected. In fact, many of today's threats don't use a malicious file at all. Phishing emails will contain commands sent to legitimate PC systems that aren't flagged as a virus or malware. Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions.

Call us today if you're worried about your business's cyber security.

Tech Fact!

You know when you think your phone has vibrated in your pocket, but when you pull it out... nothing? This has a name: "Phantom Vibration Syndrome"

DID YOU KNOW?

You might have a RAT?

Malware gets some funny names and acronyms. One you might have heard of is the RAT – which stands for Remote Access Trojan.

It's good when your IT partner remote accesses your computer. You can watch what they're doing. But with a RAT, cyber criminals have secret remote access and you have no idea.

They can watch what you're doing, copy your passwords and launch a ransomware attack.
The simplest way to avoid a RAT is to never download files from sources you don't trust, or open email attachments from strangers. Make sure your business has appropriate cyber security software and regular training for your team.

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

In today's landscape of smart devices and computers in our pocket you would think that we've nailed the whole cybersecurity thing right?

But every day more and more people are tricked into visiting malicious websites, giving up personal information through social engineering and getting their re-used passwords compromised.

As unbelievable as it may sound, it's not only our senior citizens falling prey to these cyber-criminals, it's our younger generations as well. You would expect people 25 and under to be more tech saavvy, and that's precisely the problem, they think so too.

But you're OK right? You have the fancy firewalls and antivirus with all the bells and whistles.

But what about Security Awareness Training? Oh, you have that during employee onboarding? That's great! But what about the rest of the time?

Security Awareness Training needs to be a year-long endeavour and you need to keep your employees (and yourself) on their toes to make sure that they actually remember and apply what they learned when they started.

We can help you implement a proper Cybersecurity Awareness Training Programme, just get in touch.

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 needs.

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

Request a quote today.

Question

How can I make my display more organised?

Answer

Consider adding a second monitor. Not only will this allow you to better organise your apps and windows, but it will also give you more workspace.

Question

Can my phone be hacked?

Answer

Yes! As well as the risk of phishing and smishing (that's phishing via text message), you also put your data at risk by connecting to public Wi-Fi. Fake apps can be an issue too.

Question

How do I know if my Teams app is up to date?

Answer

Just click on the three dots next to your profile picture and select 'Check for Updates' from the menu. If you're using Windows 11, you'll need to check under settings -> about Teams.

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