Understanding Cyber Security

datacentreplus

www.datacentreplus.co.uk

Cyber Security

What is Cyber Security

Cyber Security is the process of protecting networks, your data and your devices from hackers and other individuals who want to steal information or cause damage to your IT systems.

There are many ways to prevent and mitigate against cyber threats and having a good cyber security policy is an essential first step organisations should have to protect their systems and data.

Who are Datacentreplus?

We are a Manchester-based hosting and data centre services company. We provide core IT services to companies ranging in size from SMEs to Enterprise and from industries as varied as digital marketing, retail, logistics, manufacturing, web development, network services and hospitality. We pride ourselves on the personalised service we provide to all of our customers, irrespective of their size.

We deliver our services from our privately-owned, secure, ISO27001-certified data centre in Manchester, close to all major routes and public transport links.

Our core networks use Cisco equipment and the facility has 24x7 intrusion detection and environmental monitoring in place for your peace of mind.

Our highly capable team are experts in their fields but, more importantly, they are approachable, responsive and relish getting to know customers, providing you with the best possible service.

Table of Contents

Firstly, what is Cyber Security and why is it important?

Cyber security comes in different shapes and sizes and can be both physical (for example, firewalls) and behavioural habits (like remembering to change passwords regularly).

The average cost of a data breach in 2021 was £85,000 in the UK.

The figure is even higher for global cyber attacks, with IBM reporting a figure of $4.24 million for 2021.

As businesses rely more and more on their IT infrastructure and data becomes ever more valuable, the cost of a cyber attack goes up. This can range from a minor breach to immense reputational damage and, in many cases, businesses never recover from it. There is a huge number - 60 Percent Of Small Companies Close Within 6 Months Of Being Hacked.

The biggest security threats remain ransomware, phishing, identity theft, remote working exploitation and software vulnerabilities. To give some idea of the numbers involved, according to ITPro, 121 million ransomware attacks were recorded in the first half of 2020 with a 20% increase in ransomware cases around the world

Cybercriminals are becoming increasingly stealthy, sophisticated and continuously evolving their methods of attack. Similarly, the best prepared organisations take the time to regularly review and, where appropriate, evolve their cyber security policies. Doing nothing is no longer a real option.

How
To Protect Yourself from Cyberattacks

Protecting yourself from cyberattacks involves providing your employees with the right education and knowledge on the subject so they have an idea on what to do and what not to do. Most cyber incidents evolve by way of human error, not a failing in technology.

Train your staff to recognize different types of attacks, such as phishing and email scams.

Enable multifactor authentication to enhance your security significantly.

Assess your vulnerabilities so you can appropriately safeguard against weaknesses.

Create a strong password. Many cyber criminals can take advantage of weak passwords.

Be cautious with online shopping. There are lots of fake and malicious sites on the internet.

Beware of scam emails and links. Phishing scams are getting harder to detect.

Update software regularly. Hackers can take advantage of security gaps in outdated software.

Be cautious of public wi-fi. When you use public wifi, files can be potentially exposed.

Security monitoring - to identify any unexpected or suspicious activity

Statistics on recent Cyber Security breaches

In 2021, the average number of cyberattacks and data breaches increased by 15.1% from the previous year. This figure increased dramatically during the Covid-19 period.

95% of Cyber security breaches are caused by lax processes and human mistakes

90% of small businesses reported cyber attacks that caused a severe impact on their business

Examples of companies hit by cyber criminals:

Yahoo - with an estimated 3 billion accounts breached, causing significant reputational damage. This happened over a long period of time and they forced all users to change their passwords and re-enter personal information into a more secure fully encrypted environment.

LinkedIn - Data associated with 700 million LinkedIn users was posted for sale in a Dark Web forum in June 2021. This exposure impacted 92% of the total LinkedIn user base of 756 million users. The hacker scraped the data by exploiting LinkedIn's API. LinkedIn claims that, because personal information was not compromised, this event was not a 'data breach but, rather, just a violation of their terms of service through prohibited data scraping.

In April 2019, the UpGuard Cyber Risk team revealed two third-party Facebook app datasets had been hacked into and were being leaked out online. One, exposed more than 533 million records detailing comments, likes, reactions, account names, Facebook IDs and more. This database was leaked on the dark web for free in April 2021, making Facebook one of the largest companies to be hacked and have peoples data exposed.

The NHS was subject to a serious cyber attack in May 2017 that is estimated to have cost the NHS £92m and the cancellation of 19,000 appointments. A Department of Health and Social Cares (DHSC) report concluded that it estimates around £20m was lost during the attack mainly due to lost output, followed by a further £72m from the IT support to restore data and systems. The NHS was subject to an attack by the so-called 'WannaCry' virus and was essentially a ransomware attack that demanded payment from various NHS trusts to secure release of data. The ransomware attack worked by causing around 200,000 NHS computers to lock out users with red-lettered error messages demanding payment in Bitcoin, and has since been blamed on elite North Korean hackers.

There are so many companies hit by cyber crime that no company can ignore the threat. People's data is still one of the most sought-after commodities and companies may think it is only the large companies that are attacked but unfortunately that is not teh case. Millions of businesses are being targeted due to them having no security and making them an easy target to get lots of information.

57%

Companies Recovered their data using a cloud backup if available

58%

Data breaches in the healthcare centre have Risen by 58%

65%

Data Victims only get over half of their data back after an attack

Safe Backup › Data Management › Speedy Restore

In the unfortunate event that you are the victim of a cyber attack, our CloudPLUS backup service is designed to recover your data quickly and securely to get you up and running as soon as possible.

Common Threat Types

Malware
Software specifically designed to gain access to a device or damage it without the owner knowing.

Exposed Application
Feeding vulnerable servers or mobile apps with malicious imputs with the objective of injecting malicious code.

Web based attacks - SQL Injection
When criminals exploit vulnerabilities in coding to gain access to a server or database.

Phishing
Attempting to intercept user names, passwords and financial credentials by combining spoofed emails and counterfeit websites.

DDoS
A Distributed Denial of Service Attempting to impair your device and intentionally hinder a program by overwhelming it with traffic from multiple sources.

Ransomware
Ransomware is a malware designed to deny a user or organisation access to files on their computer so the hacker can demand payment for the encryption key.

Man in the middle
A malicious hacker is someone that is actively working to disable security systems with the intent of either taking down a system or stealing information.

Business email compromise - Invoice Fraud
Business email compromise is a form of phishing attack where a criminal attempts to trick a person into transferring funds, or revealing sensitive information.

Cyberextortion
Crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack. Cyberextortion attacks are about gaining access to an organisation's systems and identifying points of weakness or targets of value.

To learn more about how datacentreplus can help protect your business from scammers & hackers call us or email with your questions.

datacentreplus

Help

Examples of DOs

- Review the work policies and procedures
- Be aware of phishing emails
- Use a VPN to keep safe and connect to your company website.
- Use a strong password or a 2 factor authentication process if available.
- Consider moving your work devices to a seperate network.

Examples of DON'Ts

- Ignore guidelines for a remote work policy
- Click on random links or download attachments.
- Access your company network using insecure public wifi.
- Forget to update your software on all devices.
- Don't leave your work computers on a train or in a bar and go home.

Some DOs

Some DON'Ts

How to overcome remote working cybersecurity challenges

If you want to learn more about Remote Working solutions you can head to our website www.datacentreplus.co.uk or give us a call and recieve friendly first class customer support from us.

We'll help you with advice, guidance and the provision of remote services to your current IT infrastructure, to ensure business collaboration and secure access to your workplace desktop and applications.

Improving Cyber Security Awareness

- Learn how you can improve cyber security awareness, taking the correct steps to improve employees' cyber security awareness and protect the company from any potential risk.
- Starting with does the CEO take cyber security seriously, this will help the organisation and help create a better understanding of cyber security awareness.
- Create an effective security awareness program to identify your top risks and implement the correct security measures based on the actual threats faced.
- Get your policy management up to date, add structure to company procedures, establish boundaries of behaviour for individuals to help define compliance.
- The threat is always evolving so your cyber security awareness program needs to evolve with it, conducting regular reviews of staff readiness to identify areas of weakness.

1

Contact us

Your first step will be to contact us to review your systems and analyse any threats.

2

Threat Assessment

We will carry out a review of your current cyber security policies and existing security measures.

3

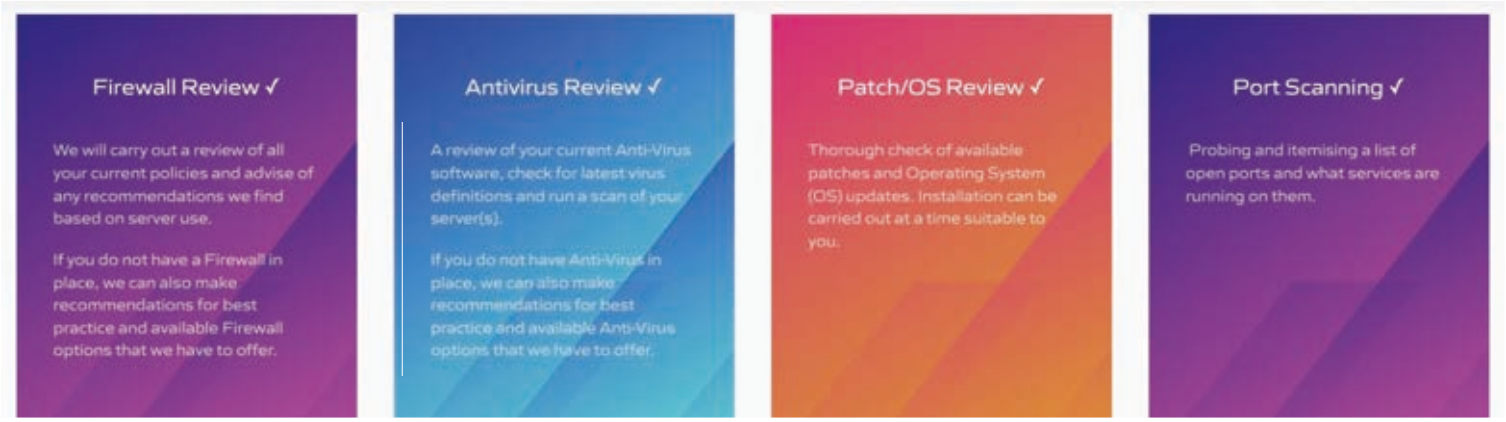
Advice and Recommendations

You will advise on best practice and improvements where necessary or recommend a more thorough review.

Why should you carry out Security Audits?

It's important for businesses to conduct Security Audits to help mitigate the consequences of a security breach and demonstrate that your organisation has taken the necessary steps to protect client and company data.

We will carry out a review of all your current policies and advise of any recommendations we find based on server use.
The Security Audits cover the following areas:



A Security Audit

Steps involved in a security audit:

1. Between the two companies, agree on audit goals. Always include all stakeholders in discussions of what should be achieved and the reasoning behind it.
2. Define the scope of the security audit. List all assets to be audited, and make sure it is all accessible.
3. Conduct the audit and identify threats. List potential threats related to each. Threats can include the loss of data, equipment or records through natural disasters, malware or by unauthorised users.
4. Evaluate and assess all risks of the identified threats, what's happening and how well the company can defend against them going forward.
5. Determine the needed controls for the business, then identify what security measures must be implemented or improved to minimise risks.

Perform an Audit

Identify security problems and gaps, as well as system weaknesses.

Stop all active threats

Review all systems and if there are threats remove them and stop them getting any access.

Protect all of your systems

Implement security processes end to end for all of your company processes.

Auditors look for weaknesses in all of your network components, highlighting areas that an attacker could exploit to access systems or information or cause damage. As information travels between two points it is at its most vulnerable. Security audits and regular network monitoring will keep track of network traffic, including emails, instant messages, files and other communications. Reviewing the network availability and all the access points are also included in this part of the audit.

Phishing

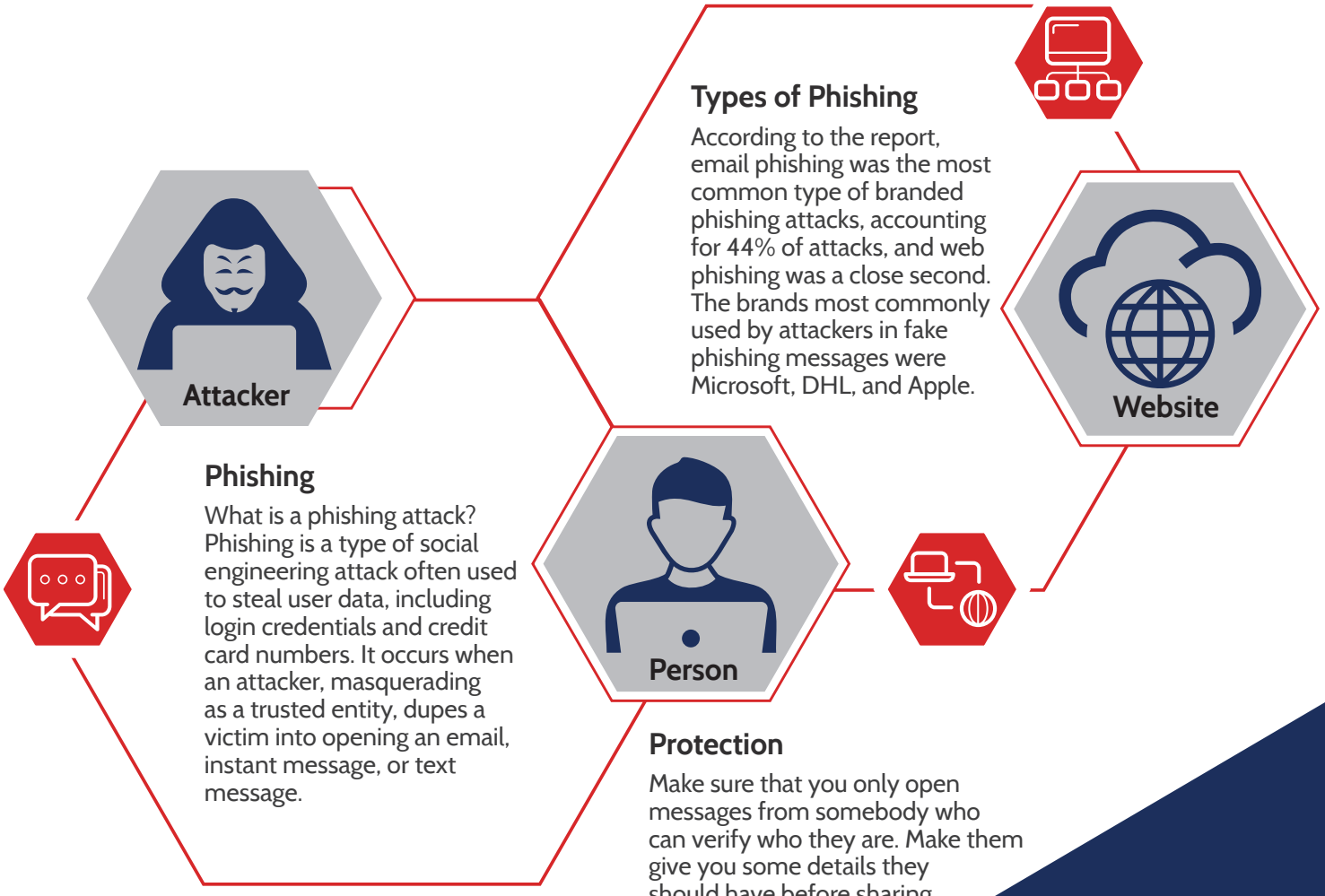
Phishing attacks are very difficult to combat. The main reason behind this is that it is difficult to track the person hiding behind their computer stealing people's information. 76% of businesses reported to be a victim of phishing last year, and that figure is likely to rise this year. How can you stop phishing attacks? If you have a secure email gateway that could help filter all the emails and remove all the spam and any that contain malicious links. There are a number of different vendors providing cost-effective, easy-to-use and highly secure email gateways that will help you to stop phishing attacks.

Deceptive phishing, With deceptive phishing, a criminal impersonates a recognised sender in order to get information like personal data or login credentials.

Spear phishing, Spear phishing is a phishing method that targets specific individuals or groups within an organization. It posses as a trusted sender that tricks a target into clicking a link that would download malicious software.

Pharming, Pharming is a type of social engineering in which criminals redirect internet users trying to reach a specific website to a different, fake site.

Google docs, Attackers use the comment feature in Google docs to email victims and lure them into clicking malicious links.



Importance of keeping your systems up-to-date

Security Breach

Server breach prevention: operating system and other software vendors will usually release software updates regularly until they decide their product is unsupported. These updates will often contain new features, fixes for bugs and performance improvements.

They will often also contain security patches and new security features, both of which it's important to install.

Patches matter because they fix known flaws in products that attackers can use to compromise your devices. New security features make it harder for attackers to successfully compromise your devices.

Without these updates, you're missing out on any potential implementation improvements for your software, as well as any entirely new features and keeping your system up to date. You might have some bugs which dispense security risks, and these can be quickly addressed with an update. Security updates can also fix vulnerabilities to new attacks that have cropped up also.

What happens if you don't update drivers?

When your computers start becoming sluggish and cause detectable performance problems that can be a serious annoyance. Device drivers are an essential piece of software that helps different hardware components work smoothly with your computer. You need to update them regularly to secure your device's performance, an outdated driver in your computer can cause your system to crash.

It's important to update your security to fix bugs and crashes, fix vulnerabilities, to ensure compatibility and to make sure cyber criminals don't stand a chance.
Here at datacentreplus we manage the risk of cyber threats, preventing the loss of revenue and reputational damage. if you want to learn more about security breach prevention you can head to our website www.datacentreplus.co.uk, we are Ideal for Digital Agencies, Small Businesses, E-commerce Sites & Web Providers!

Our team of experts take care of everything from setting your team up to making sure everything runs smoothly on your server. With our unmatched 24/7 customer support services and an experience that is tailored specifically to your needs, you can rest easy knowing it's all in the hands of our industry experts and concentrate on what really matters- your business.

Our experience and dedication keep us above the competition

What is the Cyber Essentials scheme?

Cyber Essentials
A government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyber attacks and provides a clear statement of the basic controls organisations should have in place to protect themselves.

Boundary firewalls and internet gateways
Firewalls and gateways provide a basic level of protection where a user connects to the Internet. Their role is to prevent those that are not permitted access to your network, stopping them from being able to gain control or visibility.

Secure configurations
Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.

User access controls
User access controls are a group of administration practices that restricts access to the systems, to only those that require access, guaranteeing that users are who they say they are and that they have the appropriate access to company data.

Malware protection
Malware security is a robust antivirus software which protects your devices from things like viruses and scams like ransomware and malicious websites.

Patch management
Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors such as bugs in the software.

10 types of network security

1 Network security

Network security protects the access to files and directories in a computer network against hacking; an example of network security is an anti virus system.

2 Malware protection

Malicious hackers will try and steal your personal data for personal gain. Malware protection ensures anti-virus and anti-malware systems are up-to-date and stops unauthorised access to your network.

3 Information risk regime

Information risk is an estimation based on the probability that an unwarranted user will negatively impact the confidentiality, coherence, and availability of data that you collect.

4 Monitoring

Continuously monitor all systems and networks. Look for any unusual activity that might indicate an attack. Monitoring software functions as part of firewall software or hardware and anti-virus software etc.

5 Home and mobile working

Mobile working is when staff work away from their official office base; there is a policy for all employees who work away from the office. The key to mobile working's effectiveness is ensuring employees are provided with the appropriate facilities and making sure they're safe in their environment and implementing risk assessments for health and safety concerns so they can work as productively as possible.

6 Secure configuration

Security configuration management is a process that includes adjusting the default settings of an information system in order to reduce risk and augment security.

7 User education and awareness

This is all about creating policies and providing training to employees, improving your organisation's cyber threats such as phishing and social engineering.

8 Incident management

To reduce any incidents you should produce a policy explaining what you do if you have an incident such as a security breach or a lack of access to the corporate network.

9 Removable media controls

Removable Media makes it very easy for employees to move data from system to system and it could be anything from a USB to smartphone to a DVD. To protect people from accessing your data so easily, removable media controls produce a policy to control what data people can access; the information on all appliances should be encrypted and protected with sturdy passwords

10 Managing user privileges

A user privilege enables users to perform certain actions, such as modifying database tables and monitor access to sensitive areas. Limit access to authorised people only. Privileges supply an important operational function by enabling users and reviewing their accounts, applications, and other system proceedings.

www.datacentreplus.co.uk

Tel: 0161 464 6101

Our Services

A superior hosting solution with first-class customer support

In a data-hungry world where the provision and upkeep of secure servers, storage facilities and networks are the foundations of many businesses' success, we understand that data management and hosting are more than just a contractual agreement. That's why we've built our data centre to the highest industry standards, offering the very best in physical security and resilience.

£1.3bn
UK fraud in 2021

The amount of money attributed to fraud is astrinomical. £1.3 Billion in just one year.

53.5%
inadequate security

With over 50% of online accounts not being secure it is no supprise that this threat keeps growing.

1.7 Billion
websites

There are over 1.7 billion websites and the amount of fraud attributed to these sites is growing year on year.

From dedicated server hosting, agency hosting and cloud hosting to colocation and magento hosting, we provide a vast range of solutions to meet your business objectives. Our key services are delivered from our ISO27001 certified data centre in Manchester, where access control, continuous monitoring and network protection ensure operations always run smoothly. Our specialised technical team are also on hand 24 hours a day, 7 days a week, 365 days of the year, to help with enquiries, offer advice and provide support when you need it the most.

Speak to our experts at Datacentreplus

Let us look after your systems whilst you focus on your business.

- **0161 464 6101 or hello@datacentreplus.co.uk**

Our service is always 100%

Our team are experts in their fields, but more importantly, they are approachable, responsive, and always willing to go the extra mile, providing clients with the best possible service. Whether it's offering guidance on the right RAM, necessary bandwidth or data transfer, assisting with server migration or supporting them through the tough times, we continuously prove our worth. We make things right, when it all goes wrong. That's our plus.

Our engineers are on hand 24x7x365 to help deal with any problems immediately.
Enjoy safer, faster and simpler hosting services than before. Speak to us today.

Increase of Cyber Threats

22B

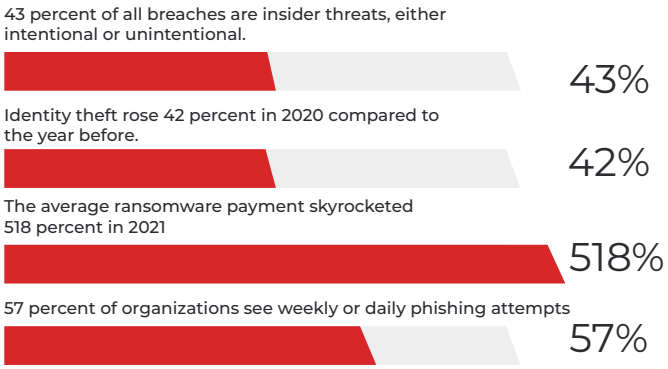
Data breaches exposed 22 billion records in 2021.

42%

Cyber fatigue, when it comes to defending against cyberattacks affects 42% of companies.

70%

70 percent of breaches in 2021 were financially motivated.



It is important to remember that 95 percent of cybersecurity breaches are caused by human error and lack of planning.

Services We Offer To Protect You From Cyber Threats

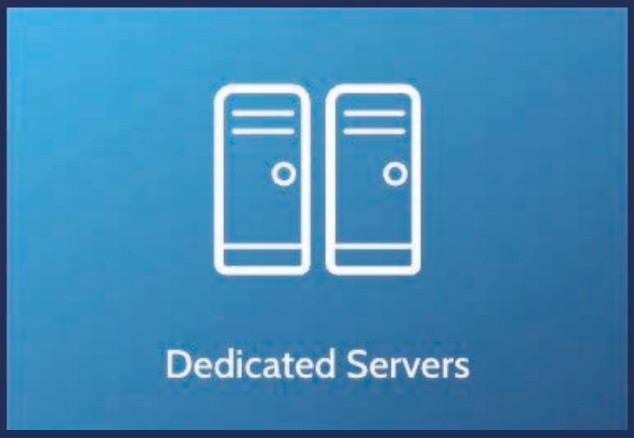
Cybercrime has many new victims, as the number of global internet users increases each year. The large rise in remote workers will continue to be a target for cybercriminals. With the ever-increasing frequency and severity of cyber threats, can you afford not to have all your computers and networks protected?

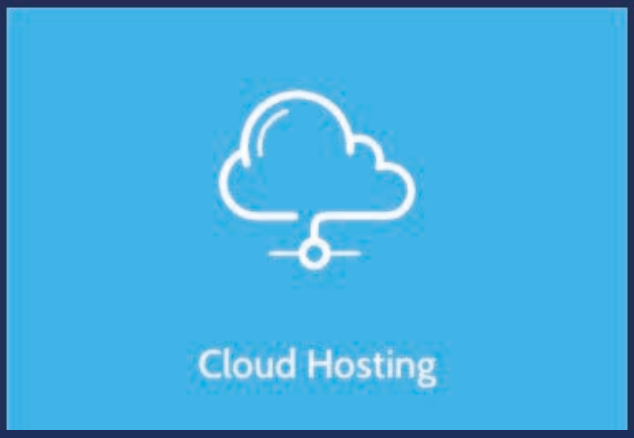
RESULTS	2019	2020	2021
Number of Cyber Crimes	668,462	697,844	847,376
Ransomware attack growth	62%	68%	73%
IT spend on security	10.7% UP	8.3% UP	13.4% UP
The average cost of a data breach	2.84m	2.9m	3.7m

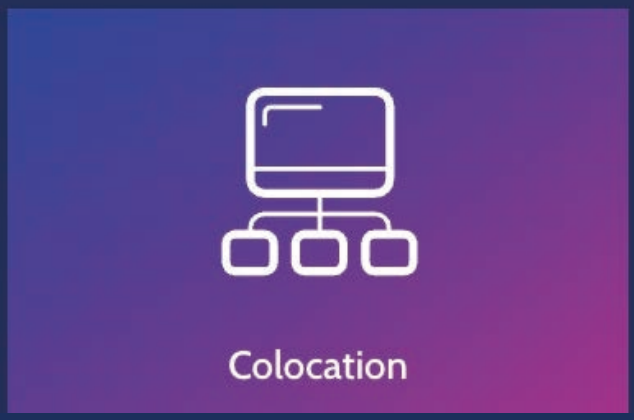
Our Services

Our team are experts in their fields, but more importantly, they are approachable, responsive, and always willing to go the extra mile, providing clients with the best possible service. Whether it's offering guidance on the right RAM, necessary bandwidth or data transfer, assisting with server migration or supporting them through the tough times, we continuously prove our worth. We make things right, when it all goes wrong. That's our plus.

We deliver our services from our own ISO27001 certified data centre in Manchester, which is secure, well-connected and regularly maintained. Our core networks use Cisco equipment that is managed by our own on-site engineers, who also, due to their expertise, provide technical support as and when necessary. We understand the frustrations of offshore call centres and useless help-desks, and therefore, we don't provide either, instead opting for support services that can actually make a difference. Even in the unlikely event of grid failures, our redundant power and connectivity systems will ensure you're always connected, allowing business to continue as usual.







Learn more about our full list of services by visiting our website.

You can scan this using your mobile phone camera.

Visit:
www.datacentreplus.co.uk

SCAN ME


datacentreplus
Trusted cloud services for your business.
To find out how we can help you, call: 0161 464 6101

CONTACT US

Get in touch with with our team to answer any of your questions about Cyber Security.

Tel: 0161 464 6101
E-mail: hello@datacentreplus.co.uk

4 Carolina Way,
Manchester
M50 2ZY

SCAN ME

datacentreplus

Certified by

HM Government G-Cloud

CYBER ESSENTIALS CERTIFIED

ISO 27001 Certified

PCI DSS COMPLIANT