
Precept IT

MANAGED IT SERVICES

Our unrivalled IT support capabilities can help all sizes of business and internal It team, no matter what your needs.

Precept IT

BELFAST BASED
SME BUSINESSES
PUBLIC SECTOR BODIES
3RD SECTOR ORGANISATIONS

Precept IT began life in 2002

Diaceutics
Better Testing. Better Treatment.

HENDERSON GROUP

GRAND OPERA HOUSE

QUEEN'S UNIVERSITY BELFAST
EST1845

Neueda™

BLK BOX

ENVISION
intelligent solutions

Catalyst

Belfast Media Group.

Dream apartments

GAA

BAUER MEDIA GROUP

ORIGIN DIGITAL

metartec
powering your future

Hill Vellacott

like

PARTTWO

MACRETE
PRECAST CONCRETE ENGINEERS

Park Hood
Chartered Landscape Architects

Napier Solicitors

Precept IT

Nexus NI
changing lives affected by sexual violence

women's aid
Federation Northern Ireland

NewLife counselling

relate
Northern Ireland

Cruse Bereavement Care

CLARE
Creative Local Action, Responses & Engagement

action mental health

SÓLÁS
teacht i méadaíocht - attaining full growth

LCCC
Lisburn & Castlereagh City Council

Woodvale & Shankill
Community Housing Association

visit Belfast

choice
Working together for positive change

cause
families, partners, friends caring for mental health

LIGHTHOUSE

domestic and sexual abuse helpline
0808 802 1414

NEW LODGE DUNCAIRN
COMMUNITY HEALTH PARTNERSHIP

MOUNT VERNON COMMUNITY DEVELOPMENT FORUM

Community Development & Health Network

LORAG
Shaftesbury
Community Recreation Centre
Balfour Avenue : Belfast

INVISIBLE TRAFFICK

Precept IT

WHY CHOOSE PRECEPT IT?

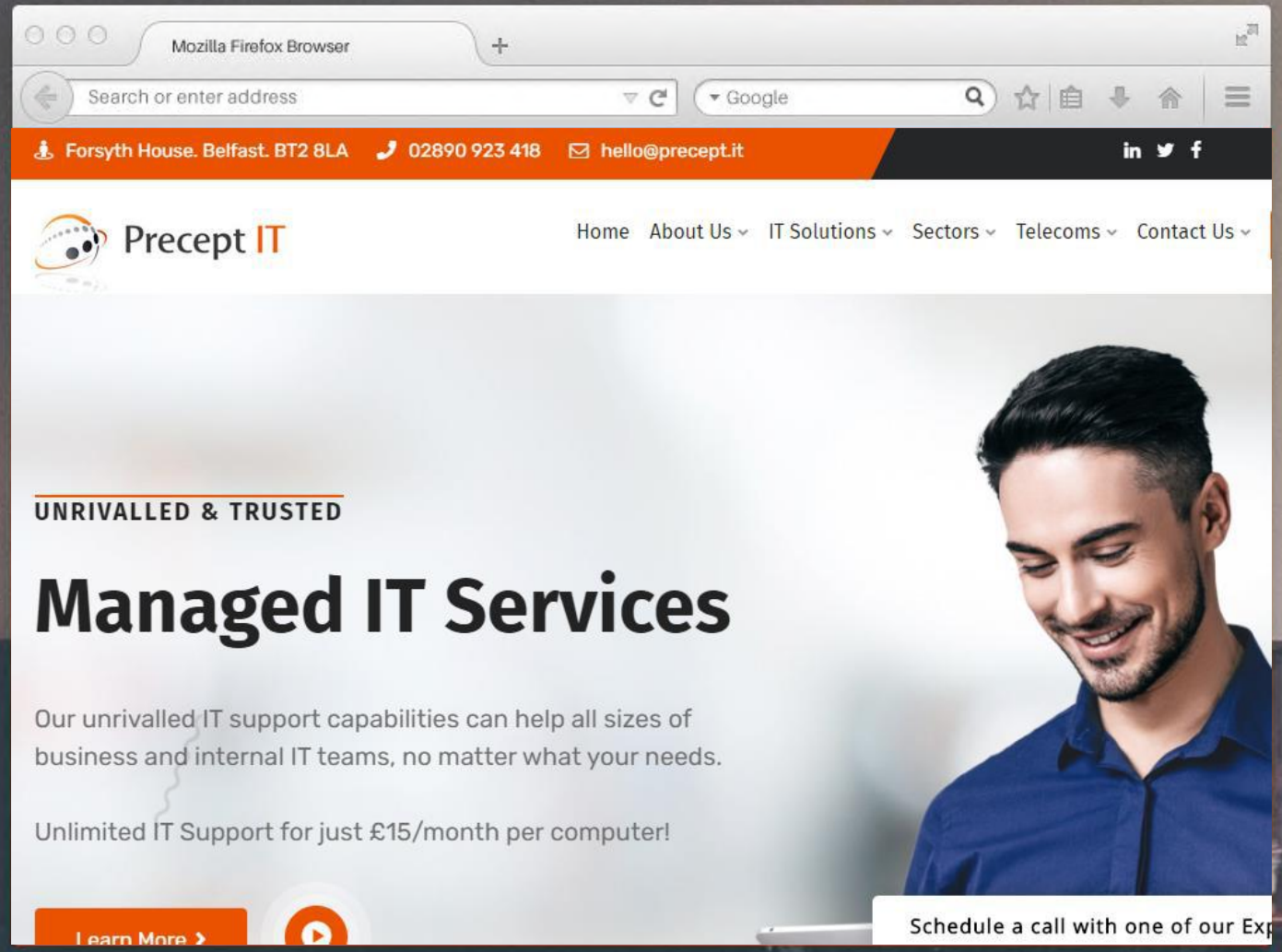
So, IT Should Just Work. Shouldn't It?

Our mission is to provide the highest levels of IT support and customer service

Precept IT

QUICK RESPONSE

95% of IT Support issues are completed remotely within 30 minutes



COST EFFECTIVE

our expertise and proactive approach keeps downtime and cost to an absolute minimum

EXPERTISE

all of our technical team are experienced, qualified and regularly trained to keep you up to date with the latest technology

EASE OF CONTACT & AVAILABLE RESOURCES

direct access to a large selection of technical staff and a dedicated Technical Account Manager

Precept IT

FLEXIBILITY & BREADTH OF SERVICE

In addition to IT Support we have a comprehensive range of network services from Disaster Recovery to IT Security. We combine our services to provide bespoke cover for all sizes of networks, budgets and service levels.

UNLIMITED IT SUPPORT PLAN

For just £15/month per computer

Fully managed contracts are your best defence against an ever-changing threat landscape. The risk to technology is growing at an exponential rate.

There are hundreds of things we do to offer assurance.

+ Control costs + Minimise risk + Secure data and information + Increase productivity + Grow your business + Provide a disaster recovery plan

Precept IT

CLOUD COMPUTING

Microsoft 365 is designed to help you achieve more with innovative Office apps, intelligent cloud services, and world-class security.

Microsoft Teams - Business Communication Platform - Go from instant messaging to secure video chat, calling & work remotely.

Vade Secure – Advanced Email Protection using artificial intelligence. Unknown email threats such as phishing, spear phishing and polymorphic malware.

BitDefender – Cloud Managed Business Grade Anti-virus, Anti-malware protection & Encryption

Acronis – Cloud backup & disaster recovery. Thwart More Security Threats, Stay Compliant and Boost Business Continuity.

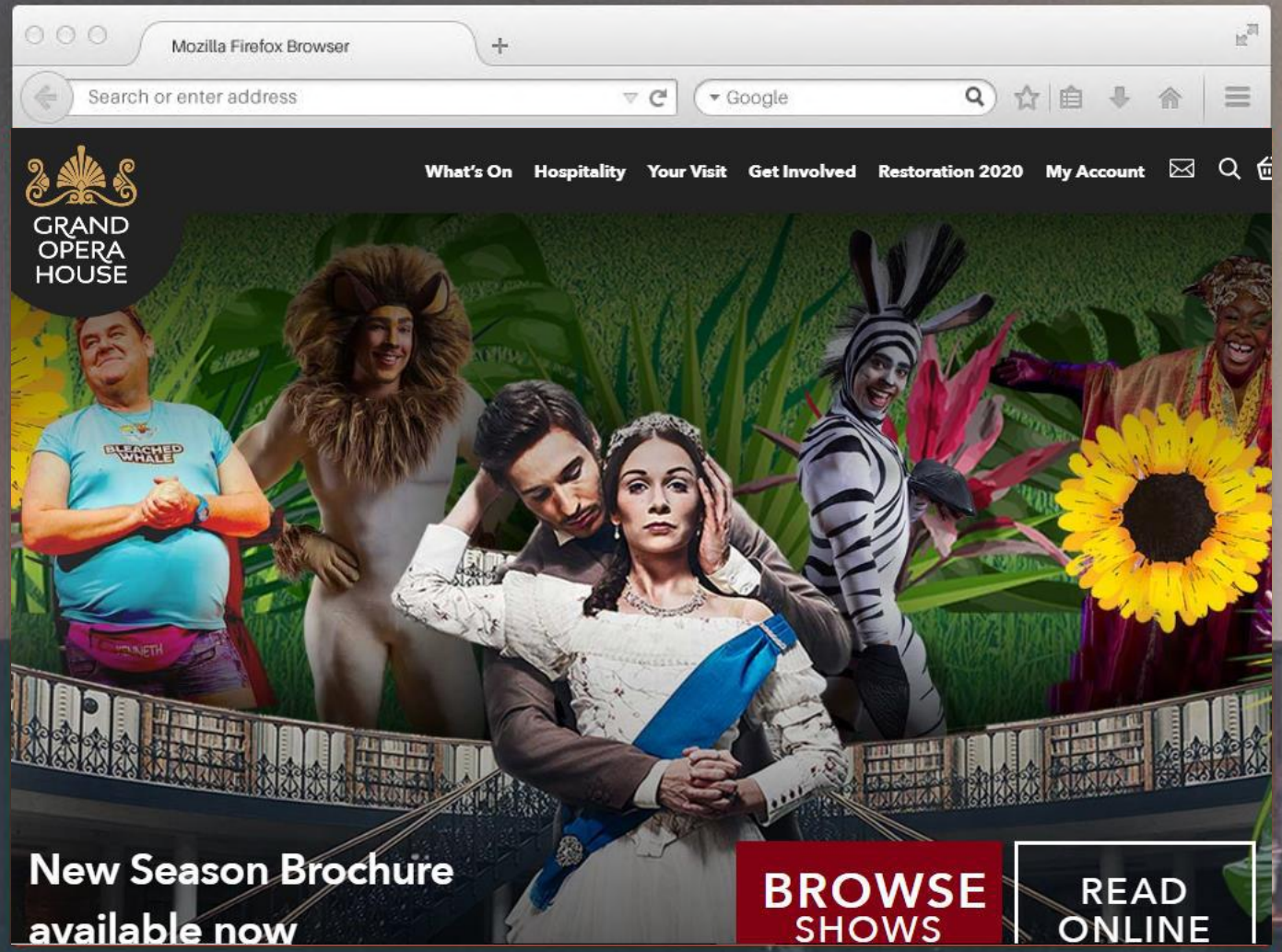
Think Backup - Managed Cloud Backup

Precept IT

PROACTIVE MAINTENANCE

+ Critical software updates applied + Anti virus software monitored + Server Disk space and health managed + Malware and spyware scanning + Monitoring Software installed and alerting enabled.

Website and Bespoke Server Hosting



GRAND OPERA HOUSE

GAA

Millennium Forum
Theatre & Conference Centre

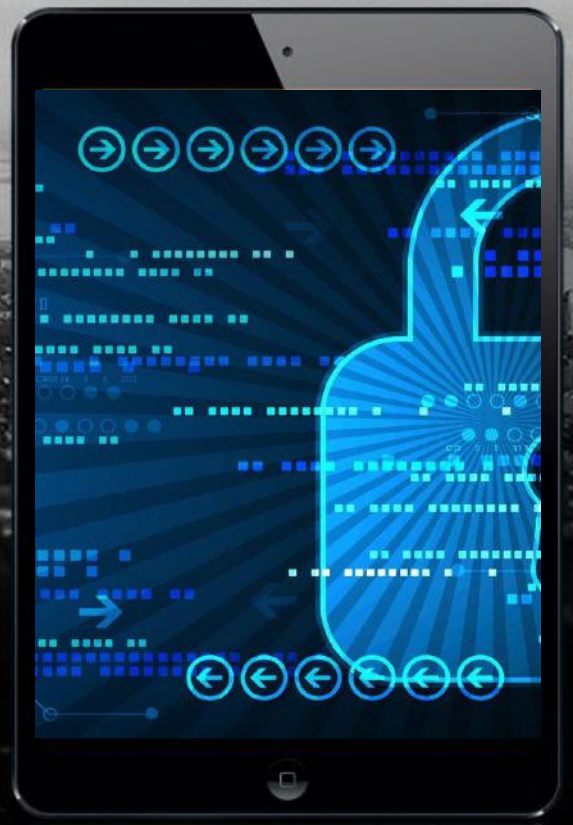
- Dedicated Virtual Server Hosting
- PHP/MySQL/ASP.net/SQL server hosting
- Backup of your files, monitoring and alerting
- Traffic Statistics and Analysis
- Search Engine Consultancy

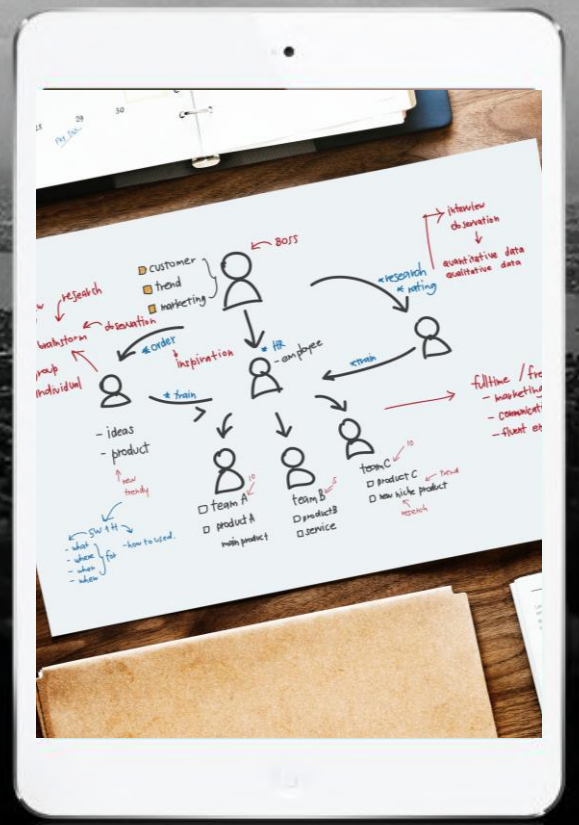
NETWORK , SERVER & APPLICATION PENETRATION TESTING

Precept IT offer a specialist infrastructure consultancy service to clients across the world.

FULL NETWORK AUDITS

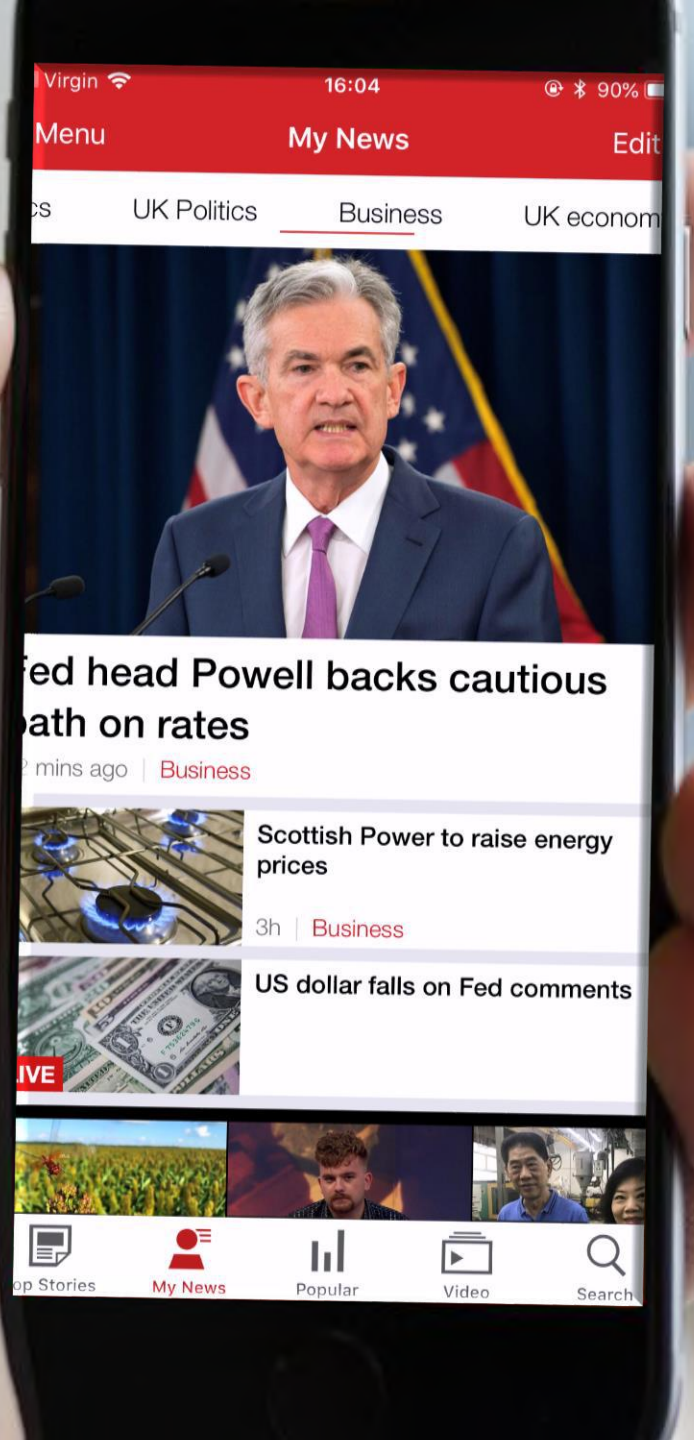
Network audit, Security and backup, Disaster recovery, Vulnerability, Ability to recover/time, GDPR compliance review, Recommendations Scope – Servers, Desktops, Wifi / Access points Firewall rules, Switches, Review of Procedures, Phone systems, Remote / mobile devices (BYOD), Applications review, Review of Backup/DR/BCP.





INTERNET ACCESS & TELECOMS

"Connect with the world in safety and with confidence. Our compliance helps secure yours."



Precept IT

HM Government

CYBER ESSENTIALS

Cyber Essentials Certified

Precept it is pleased to announce that it has been accredited with The Cyber Essentials Certification. Cyber Essentials is an industry supported scheme developed by the UK Government.

Precept IT

NO LONG TERM CONTRACTS

You'll find that most other IT Managed Services providers will tie you into contracts of three years or more, but we want to offer you flexibility.

BENEFITS

COST

The cost of bringing on an IT partner with a team of staff can very much outweigh the costs of having to directly source and hire multiple IT personnel.

IMPROVED SECURITY

Cyber-security is a big issue, with many levels and constantly evolving threats. Keeping up with, and reacting to, the latest developments is a full-time job – the job of your IT business partner.

FUTURE PROOF

An industry-expert business partner means that you do not have to worry about what changes are coming down the line, or what your business needs to do to adapt. Your business partner will have this covered.

FOCUS

With a business partner in place to manage the IT operations, time and resource is made available for you to focus on other areas within the organisation.

COMPLACENCY

If you are going to take one thing away from this presentation today,

It is don't accept complacency!

Too many businesses assume they are being looked after by there long term IT company, don't let loyalty make you a victim of cyber crime or your systems crashing.

Precept IT

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.