Contacting the Acronyms Support Desk for assistance.

If you require technical assistance please contact the Acronyms Support Desk.

Acronyms can assist with;

Poor internet connectivity
Emails on any of your devices
Working away from the office
Setting up new hardware
Installing or configuring new software
General 'how to' questions

Available Hours

Monday - Friday
08:00am - 18:30pm

Contact Acronyms Immediately

If you experience a complete loss of service or believe you are experiencing a cyber security breach.

Email: support@acronyms-it.co.uk
Phone: 01752 606 553

Acronyms

Protecting yourself from spam emails and malicious websites.

Be careful what you click or open.

Do not click on links, download attachments or respond to emails if the content is not what you'd expect to receive from the sender or if you do not know who the sender is.

Verify the identity of the other party.

Do not send money or provide confidential information at the request of an email. Verify the other party via the telephone first. Find a telephone number from a reliable source - not from within the original email.

Be wary of downloads.

Do not download files from the internet unless you are 100% certain that the website is legitimate. If you are unsure, seek a second opinion from somebody you know. You can't always rely on internet comments, reviews or videos.

Be protective of your login credentials.

Do not enter usernames, email addresses or passwords into a website unless you are 100% certain that the website is legitimate. Again, check with another person if you are unsure. Ask yourself 'Why am I providing this information?'.

Email: support@acronyms-it.co.uk
Phone: 01752 606 553

Acronyms

Basic cyber security advice and best practice.

Update regularly.

Install updates when prompted by your devices. Do not repeatedly ignore these updates, as they will contain important security patches.

Think before you click.

Make sure you know what you are clicking on. If you're not familiar with the website or the person that's emailed you, don't click the link.

Browse sensitively.

Only make online purchases, perform online banking or view sensitive data on networks you trust. Just sticking to browsing when using public WiFi.

Secure your devices.

When you walk away from a computer or laptop make sure it is locked with a secure password. Don't let devices unattended in public.

Report concerns.

If you have any concerns, ask for a second opinion or professional help. Don't make risky decisions or worry about looking foolish. It's better to be safe.

Email: support@acronyms-it.co.uk
Phone: 01752 606 553

Acronyms

Five tips for creating secure passwords.

1. Don't re-use an existing password.

Make sure your password is unique for each account that you have. This way, even if one becomes compromised the rest remain secure.

2. Use letters, numbers and symbols.

Use a mixture of different character types, as well as upper and lower cases. A strong mix of all available character types is a lot more secure than just letters.

3. Avoid personal information.

Don't make any reference to information about yourself, especially if it can be found on social media. Avoid locations, names, pets, dates and sports teams.

4. Don't use frequently used words.

Obvious words like password or letmein should be avoided at all costs. Also stay clear of sequences like abcd and keys next to one another on the keyboard.

5. Create longer passwords.

The longer a password is, the harder it is to be cracked. All passwords should be at least 12 characters long, but ideally 16 characters and above.

Email: support@acronyms-it.co.uk
Phone: 01752 606 553