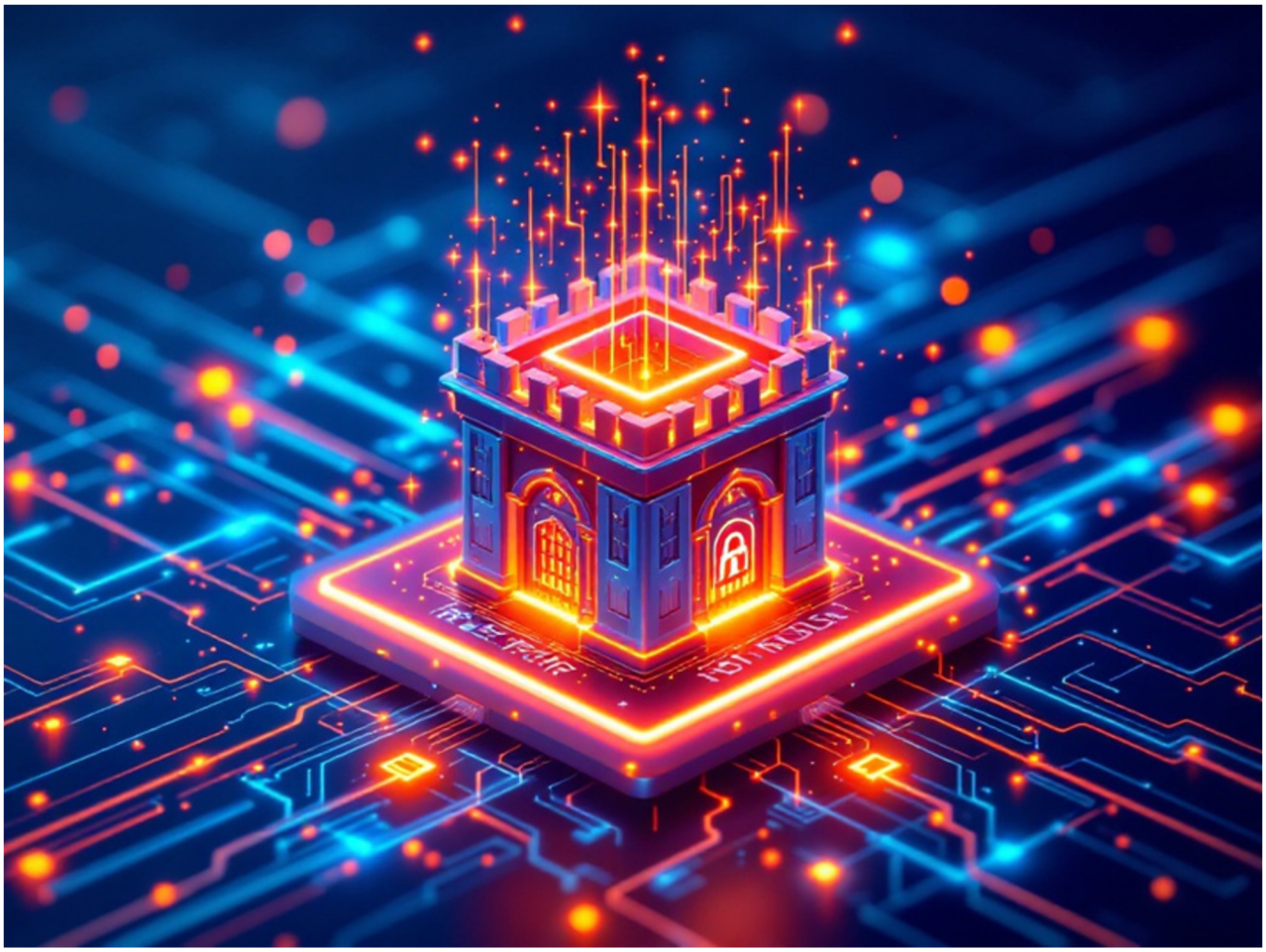

Protecting Your Business: A Guide to Basic Cybersecurity

KEYTECH
Unlock your company's potential

0113 531 5400
info@keytech.ltd
www.keytech.ltd

Welcome to Your Cybersecurity Guide

In today's digital world, cybersecurity isn't just for big corporations. We've created this straightforward guide to help protect your business from common cyber threats - no technical expertise required.

Why This Guide?

- Protect your business from common threats
- Understand basic security measures
- Learn to spot potential risks
- Keep your data safe
- Know when to seek expert help

How to Use This Guide

1. Start with the basic security checklist
2. Implement suggested measures one at a time
3. Share key points with your team
4. Keep it handy for quick reference

What's Inside:

Password Security Essentials Email Safety Tips
Safe Web Browsing Data Backup Basics
When to Call the Experts

Remember: Our team at Keytech is always here to help if you need additional support.

Essential Security Steps:

⚡These simple security measures can protect your business from 80% of common cyber threats. Start with these basics before moving to more advanced steps.

📌 Basic Checks

- Use strong passwords everywhere

Create passwords with at least 12 characters, mixing upper case and lower case letters, numbers and symbols. Think of a memorable phrase instead of a single word. For example, ‘ I love my dog Rex!’ could become ‘iLmDR3x!2023’.

- Enable Two-Factor Authentication (2FA)

Think of this as like a second lock on your door. Even if someone gets your password, they can’t get in without the code sent to your phone. Enable this on important logins like email, banking and social media accounts.

- Keep software updated

Those update reminders might be annoying, but they’re crucial for security. Set aside time each month to run updates, or better yet, enable automatic updates where possible.

- Install antivirus software

Think of antivirus as your business’s immune system - it needs to be active and updated. Make sure it’s running on all devices, including laptops that go home.

Pro Tip

Use a password manager to create and store strong passwords. It’s like having a secure vault for all your passwords - you’ll only need to remember one master password.

Staying Safe with Email

- Check sender addresses carefully

Scammers often use addresses that look almost right. ‘amazon-shipping.com’ isn’t the same as ‘amazon.com’. When in doubt, hover over (don’t click) any links to see where they really go.

- Be wary of unexpected attachments

Never open attachments you weren’t expecting, even from people you know. If in doubt, contact the sender through a different method to verify they sent it - perhaps call them on the number advertised on their website (not the one in an email footer).

- Watch for urgent or threatening messages

Scammers often create false urgency. Be extra careful with emails demanding immediate action, especially about payments or account problems.

- Keep business and personal email separate

Use your business email for work only. This makes it easier to spot unusual messages and keeps personal risks away from business data.

Browsing Safely Online

- Check for HTTPS

Look for the padlock symbol in your browser’s address bar. No padlock? Don’t enter any sensitive information on that site.

Pro Tip

If an email seems suspicious, take a screenshot and forward it to your IT Team.
Better to check than be sorry!

- Be careful with downloads

Only download files from trusted sources. If software isn't from the official website or app store, it could be harmful.

- Use work devices for work

Keep personal browsing to personal devices. This reduces the risk of accidentally downloading something dangerous to your work network.

- Watch out for pop-ups

Legitimate sites rarely use pop-ups. If you see one, especially claiming your computer has a problem, don't click - close the window.

Common Cyber Threats Made Simple

- Phishing Emails

Think of these as digital con artists - emails pretending to be someone they're not. They might look like they're from your bank, supplier, or even a colleague.

- Ransomware

Imagine someone putting a padlock on your filing cabinet and demanding money for the key. Ransomware does this to your digital files.

- Password Attacks

Like someone trying every key they can find to unlock your door. Hackers use software to guess passwords until they find one that works.

- Social Engineering

The digital version of someone smooth-talking their way past security. Criminals use persuasion to get sensitive information

Pro Tip

Most cyber attacks aren't highly sophisticated - they rely on human error. Being aware and careful stops most threats.

Need Expert Help?

Cybersecurity doesn't have to be complicated, but sometimes you need professional help.

Contact Keytech immediately if:

- You suspect a security breach
  Better safe than sorry - early detection is crucial

- Unusual pop-ups appear frequently
  This could indicate malware

- Your system seems unusually slow
  Might be more than just performance issues

- You're unsure about an email or website
  We'd rather check than clean up afterwards

Get In Touch:

📞 Call: 0113 531 5400
✉️ Email: info@keytech.ltd
🌐 Website: www.keytech.ltd

Available Monday to Friday 9:00AM to 5:00PM

Scan for immediate access to our support resources

Save our number now - because when it comes to cybersecurity, quick support can make all the difference!