Helpful terminology and tips on avoiding cyber-crime

- **Baiting** – A USB drive or another electronic media device is passed to you, which is pre-loaded with malware.
- **Clickjacking** – Concealing hyperlinks beneath legitimate clickable content, which when clicked, downloads malware.
- **Doxing** – Publicly releasing a person's information, typically retrieved from social networking sites.
- **Cross-site scripting** – When a malicious code is injected into a website.
- **Social Engineering** – A strategic use of conversation to extract information from people without giving them the feeling they are being scammed.
- **Pharming** – Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential information.
- **Phishing** – An email that looks like it is from a legitimate organisation or person, but actually contains a link or file with malware.
- **Spoofing** – Deceiving computers or users by hiding or faking one's identity. Email spoofing utilises a fake email address or simulates a genuine email address.
- **Keystroke logging (Key logger)** – Spyware that is used for covertly recording the keys struck on a keyboard. The log file created by the key logger can then be sent to a specified recipient. By examining the key log data, it may be possible to find private information such as usernames and passwords.

- **Set secure** passwords and do not share them with anyone.
- **Keep your operating system**, browser, anti-virus and other critical software up to date.
- **Verify the authenticity** of requests from companies or individuals by contacting them directly. If you are asked to provide personal information via e-mail, you can contact the company directly to verify this request.
- **Pay attention** to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net).
- **Turn off the option** to automatically download attachments on your e-mails.
- **Be suspicious** of unknown links or requests sent through e-mail or text message. Do not click on unknown links, regardless of who the sender appears to be.

Please feel free to call our helpful and knowledgeable team on 01843 572600 if you would like any advice about your security. You can also email us at hello@365itsupport.co.uk – we are always happy to help and provide advice for your IT requirements.

bcs
business computer solutions