SAFE AND SECURE IT GUIDELINES

Keep your laptop or PC locked when you are not at your desk. This can be achieved very easily by simply hitting CTRL-ALT-DEL before you intend to leave your desk, and will keep your machine locked with your Windows password until you return. This should be adhered to at all times but is especially important when we have visitors or workmen wandering around the office. Which leads into...

Be mindful of company sensitive information on display when we have visitors. It is not uncommon for customers, suppliers or workmen to visit us from time to time and sometimes they will be walking well within visibility of your screen. Be aware of any information that we may want to keep to ourselves, such as pricelists, meeting agendas, company policies, and non-work related web pages.

Keep your Windows and software applications up to date! This is a very important practice that is commonly missed or overlooked. Updating software or Windows can be a time consuming process but it is vitally important in keeping a secure network. Hackers are finding new backdoors and vulnerabilities literally by the day and software manufacturers are constantly releasing new patches to keep them at bay. Generally your software should update automatically but if you get a notification to complete an update manually – DO IT! Take a break, play some tables tennis, make a cup of tea. For more information on this, search for the Windows Update Guide on the intranet.

Keep a close eye on removable media. Storage devices such as USB sticks or discs easily go missing. Be very careful if you are storing or transporting company data on them.

Always use strong passwords. All online accounts and sensitive documents should be protected securely and to do this you need a strong password. Avoid using normal words such as “password” or “secret”, and words that could be easily linked to you such as your favourite band or sports team. Using upper and lower case characters is a simple but effective way to make your password harder to crack. Adding numbers or character symbols is another. Also make a point of changing your passwords often, at least every few months, and make sure the new password is significantly different from previous ones.

When replying to emails, always be sure to take a look at the CC and BCC fields. Some applications with email functionality don’t always make the CC and BCC fields obvious and you could end up sending email content or attachments to unwanted recipients. Be aware -- this is an easy way to get caught out.

Also be mindful of email from untrusted sources. we do have anti-spam and virus protection in place but it isn’t infallible. If you’re reading an email for the first time and something about it doesn’t quite feel right, maybe the address it came from looks dodgy or the spelling and grammar looks suspect, then your instincts are probably correct and the email should be avoided. If you are in doubt then speak to somebody in Tech Support about it and certainly do not click any links or attachments that you aren’t 100% certain about.