# St Jude's Online Safety Newsflash

Did you know that, in the UK, more than **4,000** online ransomware attacks have occurred every day since the beginning of 2017? During this time, 18 million new malware samples were captured by online protection programmes such as Norton Anti-Virus.

## Online Safety Top Tips of the Week

***Your online identity is precious. Here is how to protect it:***

**1. Don't play social media games** - one of the most notorious information security holes is *the secret question and answer*. These kinds of checks are very weak in terms of security, and are often the tool used to crack open people's accounts. It's a common game on social networks to post your "wrestler name" or "superhero name" and so on, which usually involves combining something like the name of your first teacher with the place you grew up. You've just given them the answers to two commonly asked security questions!

**2. Don't take unofficial online quizzes -** one way to check trustworthiness is to look at the URL (internet address) the quiz came from before you click it – if it's not a recognised, reputable name (like Buzzfeed), don't take the risk. But malicious sites can also disguise their web addresses, so if you can avoid it, *it's best not to do those quizzes at all*.

**3. Turn on two-factor authentication** - it might have an awkward name, but two-factor authentication (or 2FA, or TFA) is a way of adding an extra layer of security to your accounts. When you log in, you get a one-time passcode sent to your mobile phone – or even better, get an authenticator app such as Google Authenticator.

**4. Use a password manager** – you could download either 1Password or LastPass and start making random passwords for every site you use.  One further suggestion is, next time you get a new phone or a computer, *start fresh and change account passwords as you add them.*