

BASIC IT SECURITY LIST

01		<p>Ensure your passwords are strong and secure Use multi-factor authentication where possible. Regularly change passwords, and do not share them.</p>
02		<p>All devices - the latest available security updates Run weekly anti-virus and malware scans and have up-to-date security software.</p>
03		<p>Back up your data regularly Back up – not just your computer, but also your phone and your tablet.</p>
04		<p>Use a spam filter for your email Be wary of downloading attachments or opening email links you receive, even if they are from someone you know.</p>
05		<p>Use a VPN Especially if you use public WiFi, use a VPN – it ensures security. Anyone intercepting the encrypted data can't read it.</p>
06		<p>Think before you share Keep personal information private and be aware of who you are interacting with.</p>
07		<p>Monitor your accounts regularly Check your accounts (including bank accounts, digital portals and social media) for transactions or interactions you did not make, or content you did not post.</p>
08		<p>Use payment services when shopping online When shopping online it's best to stick to credit cards or payment services like Paypal.</p>
09		<p>Only visit secure HTTPS sites If you don't see the "s" at the end of "http," then the site is not encrypted and your data will not be secure. All legitimate shopping sites will have the "s" for your protection.</p>
10		<p>Don't download programs or open attachments Be sure you are downloading authorised and legitimate programs. Unless you know the program is legitimate, do not open attachments or download programs.</p>