**ATO Cyber Safety Check List**During this time of heightened scam activity, individuals and businesses are encouraged to:

1. use multi-factor authentication where possible and don’t share your password with anyone
2. run the latest software updates to ensure operating systems security is current
3. secure your private Wi-Fi network with passwords (not the default password) and do not make financial transactions when using public Wi-Fi networks.
4. exercise caution when clicking on links and providing personal identifying information.
5. only access online government services via an independent search – not via emails or SMS.
6. call us on an independently sourced number to verify an interaction if in doubt
7. educate your staff on cyber safety and scams.

To report a data breach or scam visit [ato.gov.au/onlinesecurity](https://www.ato.gov.au/general/online-services/online-security/?utm_campaign=cybersafety_2020&utm_source=pr&utm_medium=email&utm_term=checklist)