

DATA SECURITY OUTSIDE YOUR USUAL WORKPLACE.

1.



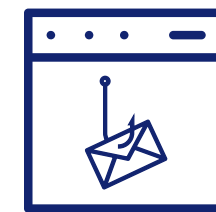
Make regular backups:
Using cloud-based or centralised storage that's remotely and securely accessible is preferable.

2.



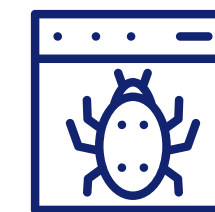
Make backups encrypted:
Ensure two-factor authentication is required to access your backups.

3.



Beware of cybercrime:
Fraudsters are making the most of fears and concerns right now and ramping up phishing emails – don't click!

4.



Allow security updates:
Malware and online threats are constantly evolving. So too is the protection against them, if you keep it updated.

5.



Password protect devices:
Use two-factor authentication and don't share passwords with anyone.

7.



Check your WiFi:

- Use WPA2.
- Password protect your network.
- Make sure you are not still set-up with the default admin username and password!
- Use a Virtual Private Network (VPN) where you can to connect between your home and business.



6.



Use complex passwords:
Passwords should ideally include a mixture of numbers, capital letters and special characters.

Data-security@elavon.com

Elavon.co.uk/security | Elavon.ie/security