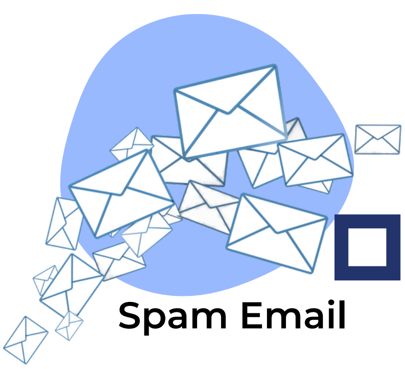
Is your business cyber-safe?



□

Spam Email

Most attacks originated in your email. Consult your IT advisor for ways to reduce spam and exposure to attacks on your staff via email.

□

Passwords

Set password policies, user screen timeouts, and limit user access, also implement business-grade Password Management Software.

□

Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM (Security Information and Incident Management).

□

MFA

Utilise Multi-Factor Authentication (MFA) whenever you can, including on your network, banking, websites, and social media. MFA gives additional protection to your online accounts.

□

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (i.e. email), and especially on mobile devices. Other additional protections are hashing and salting - ask us if you have any questions!

□

Device Update

A software update offers the latest bug fix and security patches. Consult your IT team for a 'critical update' via automation to keep your computer protected against the latest known attacks.

B&A TECHNOLOGIES

Minimise technology costs
Optimise business processes
Maximise revenue through technology

www.bettstechnologies.com

B & A Technologies Pty Ltd

B & A Technologies

□

Endpoint Protection

Endpoint security protects your devices and data from malware, viruses and cyber attacks. Works beyond anti-virus, endpoint protection technology protects against file-less and script-based threats and can even rollback a ransomware attack.

□

Cloud Security

Cloud Security stops malicious websites from stealing your logins and identity (even when laptops are used out of the office). It also prevents staff from accessing non-approved websites. A must-have for hybrid working arrangements.

□

Dark Web Research

Know in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. Consult your IT advisor about Dark Web scans and strategy to protect your business from stolen credentials.

□

Security Awareness

Your staff is the gateway to your most valuable assets - your data. Train your staff and teach them about data security, email attacks, and policies and procedures. How about running a simulated Phishing Campaigns? We can help!

□

Security Assessment

It's important to establish a baseline and mitigate existing vulnerabilities. When was your last assessment?

Last Assessment Date:_______________

Next Assessment Date:_______________

Did you know?

1 in 5 Australian Small and Medium Businesses (SMBs) did not know the term “phishing”.

$300 M Estimated annual losses to cybercrime based on ReportCyber data.

Results from the Australian Cyber Security Centre Small Business Survey