ASB
ONE STEP AHEAD

Helping you protect your business from fraudulent activity and scams

Five steps on the path to being more secure:



1. Assess your online security

- If you don't have an IT Manager, give someone responsibility for your network security. Remember it's everyone's responsibility to comply with your security procedures.
- Complete a self-assessment against the CERT NZ Business Guides.



2. Develop an online security policy for your business

Your online security policy sets rules to protect your business. It includes simple security controls for the ways you and your team use your systems and devices.

Hold regular company meetings designed to remind staff why information security is important.



3. Establish an incident response management plan

Your incident management plan gives your employees guidance on recognising and dealing with a cyber security breach. You can also find guides on Cert NZ to help you plan and prepare.



4. Keep informed

Subscribe to security notification services, like Cert NZ that keep you informed about the latest online safety and security risks and solutions.



5. Review your security regularly

Once you've set up your risk management approaches, you need to make them part of your culture.

For more advice you can also refer to information on our website;

asb.co.nz/business-banking/guidance/keeping-your-business-safe-with-cyber-security

ASB
ONE STEP AHEAD

Actions to help protect your business banking



Business Email Compromises

- Ensure staff are trained to recognise suspicious emails
- Ensure you have clear policies around authorisation of payments
- For new payment requests or if a regular supplier changes their account details, confirm invoice details and account numbers directly with suppliers using a phone number known to you or publicly available
- Be cautious when emails request urgent or confidential action be taken
- Put in place a 'two person rule' around signing off transactions and set transfer thresholds
- For internal payment requests by email, ensure staff personally speak with the colleague requesting the payment on an already identified contact number held by the business
- Include reminders about payment policies and procedures in your regular staff meetings



Keeping your FastNet Business Site safe

- Ensure staff NEVER share FastNet passwords or Netcode numbers
- Ensure staff use strong passwords, never write it down or give it out to anyone
- Never click on a link to access internet banking
- Consider IP Address Verification as added security - Customers need to have a fixed IP Address and can lock down anyone using FNB to only access via that IP Address
- Have an FNB segregation of duties policy for the users (for example, a user can create a payment but not authorise or a user can authorise payments but not create)
- Review daily account limits
- Regularly review your FNB admin / users still have the relevant permissions to fit their role, including daily limits, account access and permissions. There is a report under the administration section that will provide this data
- Removing a signatory from your bank accounts does not automatically remove them from FNB, you will need to do this separately
- Regularly check the FastNet Business Audit (under Administration > Client > Audit Log) to identify any unexpected changes to account numbers, extra payments or logging in after hours
- Set up Alerts to advise if a large payment is deducted from an account or if the account goes into overdraft

If you want to review your security for FastNet Business phone our Helpdesk on 0800 225 527

If you suspect you are being scammed or your account security has been compromised, contact ASB immediately on 0800 803 804 or your account manager.

asb.co.nz

ASB Bank Limited 6180 17289 0720