Internet Banking for Business security essentials – managing payment security

There are several ways you can provide additional security for your business and meet your internal governance needs with Internet Banking for Business. These include:

- Setting transaction and user limits to help manage risk and prevent unauthorised payments.
- Creating user roles and permissions to help control user access and implement segregation of duties where needed.
- Adding an extra layer of approval with two-to-authorise before payments are processed.
- Turning on notifications to stay informed with alerts on account activity.
- Maintaining visibility of any new users and changes to users including changes to their limits and passwords using audit logs.

Tip

We recommend that you review your Internet Banking for Business security setup regularly. Delete inactive users, and review user roles, authorisations and limits.

To find out more visit our Help & Support page on bnz.co.nz

Limits

Setting limits allows you to control the amount that can be paid out of your accounts for specific payment types like bill payments, direct credit, payroll, and more.

Limits include:

- Daily limit – the maximum amount that can be paid out in one day for a particular payment type.
- Transaction limit – the maximum amount that can be paid out in a single transaction for a particular payment type.

You can add further controls by assigning user limits to ensure that individuals only create or authorise payments within their authority level.

Why do limits matter?

- Limits help safeguard payments paid out of your accounts per day.
- Limits prevent bulk or batch payments from exceeding agreed thresholds.
- User limits ensure individuals only approve payments within their authority.

Two-to-authorise payments

To help keep your payments secure and aligned with your business controls, you can set higher-risk payments to two-to authorise. The number of authorisers required is specified at a payment type level.

Choose the number of authorisers required based on your risk level and business needs. For example, one authoriser for funds transfers between your accounts, but two-to-authorise higher-risk international payments.

Why choose two-to-authorise?

- Adds an extra level of authorisation for higher-risk transactions.
- Helps to ensure compliance with internal controls and may reduce fraud risk.
- Provides an extra layer of quality control to identify errors, such as incorrect account numbers or payment amounts, before the payment is finalised.

Roles and permissions

User roles and permissions let you choose what users can see and do. There are eight templated roles that cover most businesses' day-to-day banking activities and permissions can also be customised for each user.

For example, some users can be assigned to create payments only, while others can be assigned to authorise payments only.

Why do roles and permissions matter?

- Segregating roles makes it harder for an individual to commit and conceal fraudulent activities.
- Involving multiple people adds a 'second set of eyes' to identify and correct errors.
- For higher-risk payments, you can combine segregation of duties with two-to-authorise rules for extra security.

Notifications

Email notifications like Account Balance, can help give you real-time visibility into your accounts enabling you to quickly spot balance fluctuations and respond promptly if something looks suspicious.

Audit log

Audit log provides visibility into user activity and system changes, helping you monitor for internal governance and protect against fraud.

You can see:

- details of newly created users
- changes to user settings, including new transaction limits and password changes
- login activity, including time and location
- whether access was via a mobile phone or a computer.

Why do audit logs matter?

- Audit logs provide early detection of suspicious activity such as unusual login attempts, which can indicate a security breach.
- They help you trace and investigate potential fraudulent behaviour.

Security tips:

- **Create unique passwords:** Change your password regularly and do not use passwords across different accounts.
- **Don't share login credentials:** Never tell anyone your password, including bank staff – legitimate BNZ staff don't need to know your password and will never ask you for these details.
- **Monitor accounts regularly:** Check your account balances and transaction history frequently to spot any unusual activity.
- **Secure your devices:** Install and regularly update antivirus and anti-malware software on all your devices used for Internet Banking for Business. Keep all operating systems and banking apps updated to patch security vulnerabilities.
- **Avoid public Wi-Fi:** Public Wi-Fi networks are often unsecure and can be easily monitored by hackers. Avoid accessing your bank accounts or making payments when connected to public networks. If you're with 2degrees, Skinny, Spark, or One NZ you'll get free mobile data when you're accessing BNZ apps, online banking, and our website from your mobile device in New Zealand.
- **Report suspicious activity:** Contact BNZ immediately, if you notice any unauthorised transactions or suspect any user's details have been compromised.
- **Learn to identify common scams:** Visit bnz.co.nz/about-us/online-security/latest-scams to learn more about common scams that could impact your business, what do when you spot them, and how to respond if you've been scammed.

bnz

Internet access required for Internet Banking for Business. Internet Banking for Business terms and conditions apply. Maintenance sometimes required.

(16268) 03-26