Security Tips in ANZ Transactive — Global

The threat of online scams and fraud in recent times is something we all need to be mindful of. We have compiled 10 actionable and practical tips you can follow to stay secure whilst using ANZ Transactive — Global.

Customers outside of Australia and New Zealand may not have access to the Administration entitlements covered in this video. Speak to your ANZ representative if you would like to review some of the tips covered.

Tip #1: An effective measure to maintain application security is to use multi-factor authentication when accessing and performing high-risk tasks such as payment approvals.

Tip #2: Review payment alerts that highlight potential duplication of payments and modified beneficiary details.

Access this by selecting Payments, then Current Payments. If an issue is identified, the payment will display an alert symbol. Click through the payment for the alert message.

Tip #3: Enable email notifications that advise of any ad-hoc beneficiaries used, transactions pending authorisation and all beneficiary updates.

Click your name on the top right-hand of screen and enable settings from Notifications and Alerts.

Tip #4: Set your Administration Model to be either dual or triple. With dual, administrators can modify their own permissions but require a second Administrator to approve the changes.

With Triple, an Administrator cannot modify or approve changes to their own permissions.

If your organisation is in Australia and New Zealand you can update your Administration Model by downloading and submitting the Amend Digital Channel Details form. Click Service Requests, Upload Documents, New, then Amend Digital Channel Details. Alternatively, you can update your Administration Model by contacting your ANZ representative.

Tip # 5: Permanently delete or temporarily disable any users who are on leave, or have left the organisation, to prevent unauthorised use of their profile.

To disable a user, click on the Administration menu to go to User Management. Right-click the user’s profile and click Disable.

Tip #6: Regularly review your Company Managed users’ contact details to avoid authentication and authorisation breaches.

Select the user from the grid and click Edit. All fields under User Details can be amended with current contact information for the user.

Tip #7: Review your users' daily, batch, transaction payment approval discretions and user access to minimise funds lost from unauthorised transactions.

To amend user discretions, click on Permission Settings near the user's role/s and update the assigned discretions.

Tip #8: Prevent unnoticeable single user transaction processing by enabling 'two to approve' or a Panel (explored later in this video) and entitle your users to 'Create & Approve (Not Own)' or other custom-created roles, further preventing a user to 'self-approve' their own transactions.

Click Add Permissions in the User Management screen, then select an appropriate role and click Continue. Select the appropriate Permission Settings and click Add Permission to assign the role to the user.

Tip #9: Set up Authorisation Panels to enforce a payment approval sequence, allowing nominated users to authorise transactions in a set order that avoids autonomous payment signing.

To create a Panel, click the Administration menu, then click Other Settings. Click New under Authorisation Panels, then populate the Panel Details, including Panel Name, Panel Currency and Panel Description.

Nominate your desired Threshold Maximum Amount and select the Panel Authorisation Groups. Under the Order drop-down menu, select the order in which approvers in their assigned panel authorisation groups approve payments. Click Submit to send the Panel for approval.

To assign a Panel Authorisation Group to your user, click on User Management, right-click on the user, select Edit and select the Panel Auth Group from the drop-down menu. Click Save on the top left-hand corner to finalise all updates on your user's profile.

Tip #10: Select the options to Disable Beneficiary Bank changes for Payments created from Templates and File Imports to avoid any unauthorised redirection of funds.

Click Administration, Other Settings, right-click on the relevant Division, click Edit, tick desired Product Settings and click Save.

For more security tips, and additional information about tips covered in this video, please refer to the Digital Services Security Features article in ANZ Digital Services Help.

To report fraud, contact our Customer Protection team: Australian customers can click Contact from the ANZ Transactive — Global banner, choose Australia from the drop-down list, click Report Fraudulent or Unusual Activity, dial the unique phone number and enter the One Time Access Code when prompted.

For all other jurisdictions, choose your location from the drop-down menu, click

View list of global contact and choose your jurisdiction and contact method for your enquiry.

REMEMBER

Verify Communications:
ANZ will never ask for financial details, OTPs (One-Time Passcodes), or account changes via email, text, or phone. Always use official contact points to verify and unusual requests.

Avoid Unverified Links:
Do not click on links in unsolicited emails, texts, or popups. Use trusted sources to find ANZ logon pages and confirm any requests.

Exercise Caution:
Be skeptical of unexpected and urgent requests, even from known contacts. Always check email addresses and maintain strong security practices.

For more information on Security Tips in ANZ Transactive – Global, visit ANZ Digital Services Help.

Help.online.anz.com
www.anz.com.au/security/latest-security-alterts/