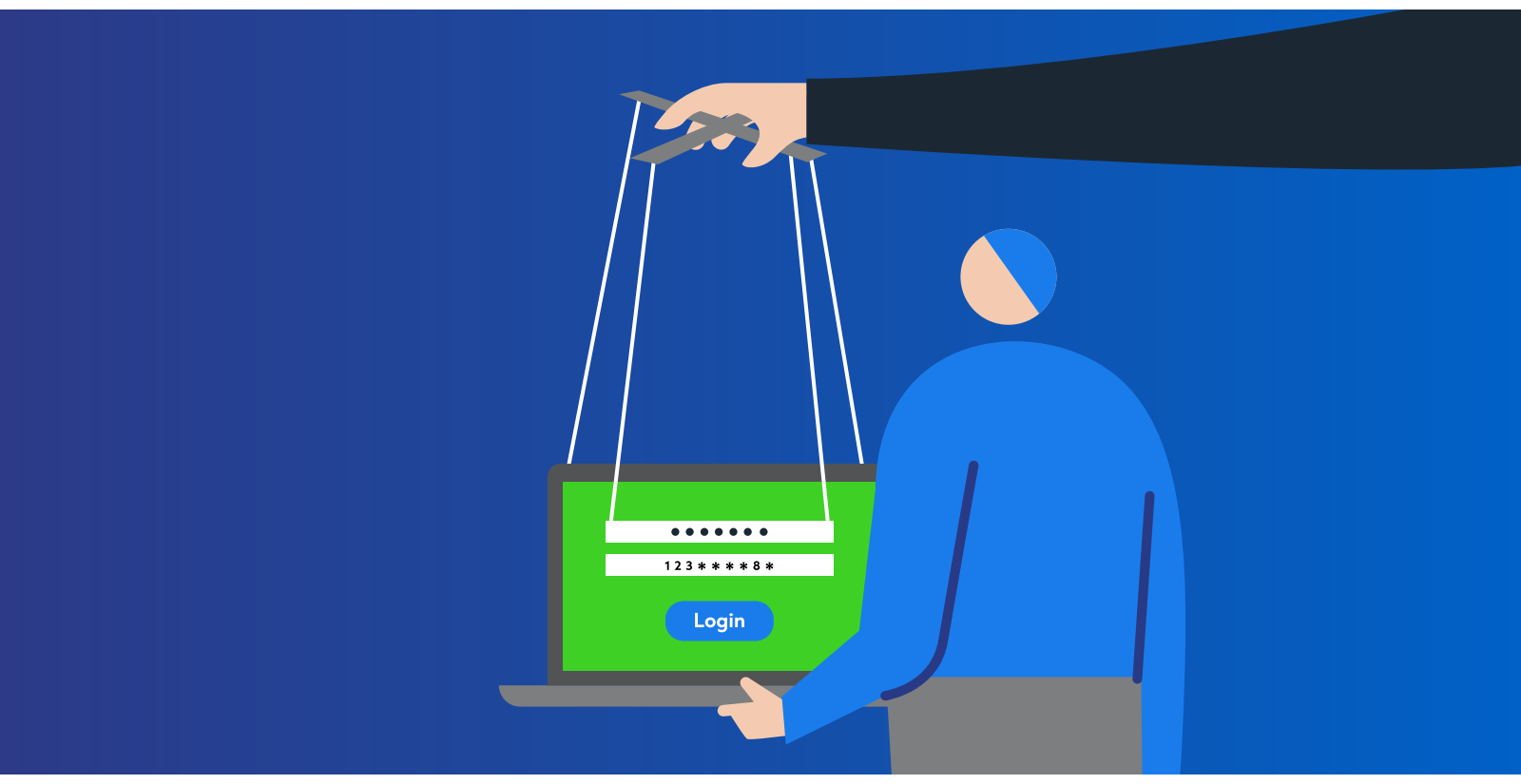

Account takeover: don’t let it happen to you

Account takeover is a form of identity theft where fraudsters successfully gain access to your banking services and accounts to steal funds or information.

What happens when an account is taken over:

Fraudsters will attempt to change your banking login credentials or contact details and you may no longer have access to your account

You may receive alerts on transactions you did not make or notice you have lower account balances or discover funds are missing from your account

You may notice disruptions to your mobile services. Fraudsters may also divert or intercept messages or calls to your phone

Fraudsters may also takeover your email accounts to gain access to your email contacts to ask for financial help, intercept sensitive emails such as bank alerts or even access important documents

Some tips to help you stay safe:

- Use **strong alpha-numeric passwords** for each of your accounts and change them regularly
- **Be careful when sharing your personal information** such as date of birth, passport or identification card number
- In the event of any disruption to your mobile service, **notify your provider immediately**
- Ensure your devices have **up-to-date anti-virus software and firewalls** installed
- **Don't click on links** in unknown or suspicious emails or messages, shop on unfamiliar websites or using unsecured public wifi networks

Be vigilant! Regularly check your account history for any suspicious or unauthorised activity. Notify your bank or the service provider immediately if you suspect your account has been compromised.