Account Takeover

Account Takeover

What is Account Takeover?

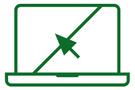
This type of fraud happens when a fraudster gains access to your bank account, typically by tricking you into divulging information, and resets your passwords and any security numbers so you cannot access your account. They may change the phone number, address and email address connected to the account; this enables them to use the account as if they were a legitimate customer.

Remote Access Takeover

This type of fraud happens when a fraudster takes control of your device and uses this control to make payments from your bank account without your knowledge or authorisation. This will usually happen after the fraudsters have sent you a link, asked you to visit a website or download a piece of software, which helps them to remotely access your device. By reading through this guide, you'll learn the tactics fraudsters use and know what you need to do to stop yourself and your business falling victim.

Number spoofing

This is where fraudsters change the caller ID (the number they're calling from), to clone or nearly clone an official number that may belong to your bank. The number may appear exactly the same or might be different by just one digit. Alternatively, they may call you from a withheld number.



Malware and Phishing

Fraudsters will use malicious software and links to steal personal information.

This information will be used to trick you into thinking a call may be genuine, or, used to hack into your bank account.

Authorisation codes

No-one, including your bank, will ever instruct you how to use your physical or digital security device (also known as your secure key) or ask you for online banking authorisation codes.

Account Takeover

Recommended Tips

- Never give out your Online Banking usernames, passwords, authorisation codes, or any One Time Passcodes (OTPs).
- Remember numbers can be spoofed and never rely on the caller ID to know who’s calling.
- For unexpected calls, don’t be afraid to return the call using an independently verified number, such as one from the caller’s official website. Use a different phone or call a known contact first to be sure the line is ‘clear’.
- Be wary of suspicious emails and text messages. Especially those which contain links and ask for information. Always validate these requests with the company directly, using the contact guidance above.
- Never click on any links, visit web addresses, or download software because of a phone call you weren’t expecting.
- Your security device, or secure key, is personal to you. If someone calls and asks you to use this device, end the call and contact your bank immediately.
- HSBC will never ask you to participate in an ongoing investigation, advise you how to answer questions or ask you to send your money to a safe account.
- Make sure you have a company procedure for staff to escalate concerns and ensure everyone in your business is aware of Remote Access Takeover fraud.
- Educate your staff – make sure everyone is aware of Remote Access Takeover fraud and have an escalation process in place.
- Incorporate a robust due diligence culture in your business for any payments which may include a two-tier approval process.