How to avoid being a victim of bank fraud

savings champion.co.uk

www.savingschampion.co.uk
0800 321 3581

Introduction

The use of fraudulent techniques to access individuals' bank accounts have become increasingly sophisticated, with the use of technology, however there are simple ways to combat this.

The following guide explains the techniques employed by fraudsters to highlight where you may be vulnerable and also provides valuable tips on how to prevent this.

Current Account/Savings Account

- Current accounts allow for far greater accessibility than savings accounts, which makes them less secure.
- At Savings Champion we regularly encounter savers who hold in excess of £100,000 with one bank. There are numerous reasons for this;
    - A historic relationship with a particular bank
    - Business sale
    - Inheritance
- Often the saver has no concerns regarding the financial strength of the individual bank and therefore feels their exposure to risk is limited.
- Savings Champion's advice in these circumstances is to consider how much needs to be held on a current account and consider transferring excess funds to savings accounts. We can assist in this process – please call 0800 321 3581.

Tip 1

Do not hold too much money in a Current Account. Try and spread it around by using Savings Accounts.

Voice Phishing

- These are unsolicited phone calls from fraudsters which encourage you to give out your personal details, such as your card, PIN or card reader codes. The fraudsters can pretend to be your bank, the police, or any other official company.
- Sometimes you may get a 'warm up call' where no information is discussed. This is to set the scene for a later call where you may be asked for information.

How to avoid becoming a victim of voice phishing

- Never give your full PIN or Digital/Telephone Banking login details to anyone, even a caller claiming to be from your bank or the police.
- If you get a call asking you for this information, end the call immediately.
- If you receive a suspicious or unexpected call, always verify the caller using an independently checked phone number such as a contact number from your banks website.

Tip 2

If you receive a call that you believe is fraudulent any call you make after the call should be from a different number (e.g. a mobile number).

- Be aware that fraudsters use techniques to hold your phone line open. When you try to dial out to verify the caller, the fraudster may stay on the line, play a fake dial tone and claim to be the person you're trying to contact. To avoid this, use a different phone line to verify the caller where possible. If not, try calling a friend or family member first to make sure your line is clear.

Contact Savings Champion on 0800 321 3581

Email Phishing

- You receive an email that looks like it comes from your bank asking you to log on and check your account. It looks real, so you might be tempted to click on the link and enter your user ID and password into the website.

- If you do you will be handing over your details to a fraudster who wants to take your money.

> Tip 3
>
> Banks will never send you an email, text or a website link asking you to enter your internet banking or card details.

Impersonal greetings and probing questions

- A phishing email may not be personally addressed to you but may begin with 'Dear valued customer'.

- The fraudster or fraudulent website may ask for sensitive personal information such as passwords, Internet banking log on details, contact details or credit card numbers.

Urgent warnings

- A phishing email may say things like 'we need to verify your account information' to try and get you to respond without thinking.

Bad spelling and formatting

- The wording of the email may have poor grammar and spelling.

- The fake website may look slightly different with an alternative layout or misspelt words.

Tips on avoiding phishing attacks

- Limit the amount of personal information you make public on the Internet, including social networks. It could be used against you.

- Treat all email with a degree of caution. The sender's or return address can be faked. The email header and website link can also be manipulated.

- Don't use a link in an unexpected or suspicious email to get to any webpage. Type the website address into your browser's search bar. Banks should never provide a link from an email directly through to your Internet Banking log in page or to a page that asks for your security or personal details.

> Tip 4
>
> In emails, website addresses may appear genuine on first sight, but if you hover your mouse pointer over the link without clicking, it may reveal a different web address

Six Steps to prevent being a victim of fraud

1

Don't listen to anyone who asks you to transfer money from your account. Banks will never ask you to take such action.

2

Don't believe anyone who says they will call back from a number that matches your bank's customer service department. The number shown on your phone can be altered by the caller.

3

Don't assume any caller is genuine simply because they have information about you and your account details.

4

If you receive a call from your bank's fraud department, you should agree to call them back using the number on the back of your bank card – preferably from a different phone.

5

Never disclose the four digit Pin number for your bank cards to anyone, including the bank or police, and do not write it down anywhere. A PIN number is private to you and should remain so.

6

If you think someone is suspicious just hang up. Clear the line by calling a number you know, or use a different phone, and call your bank.

If you have any queries regarding your savings please call us or complete the attached form;

https://www.savingschampion.co.uk/50-pound-challenge/

Contact Savings Champion on 0800 321 3581