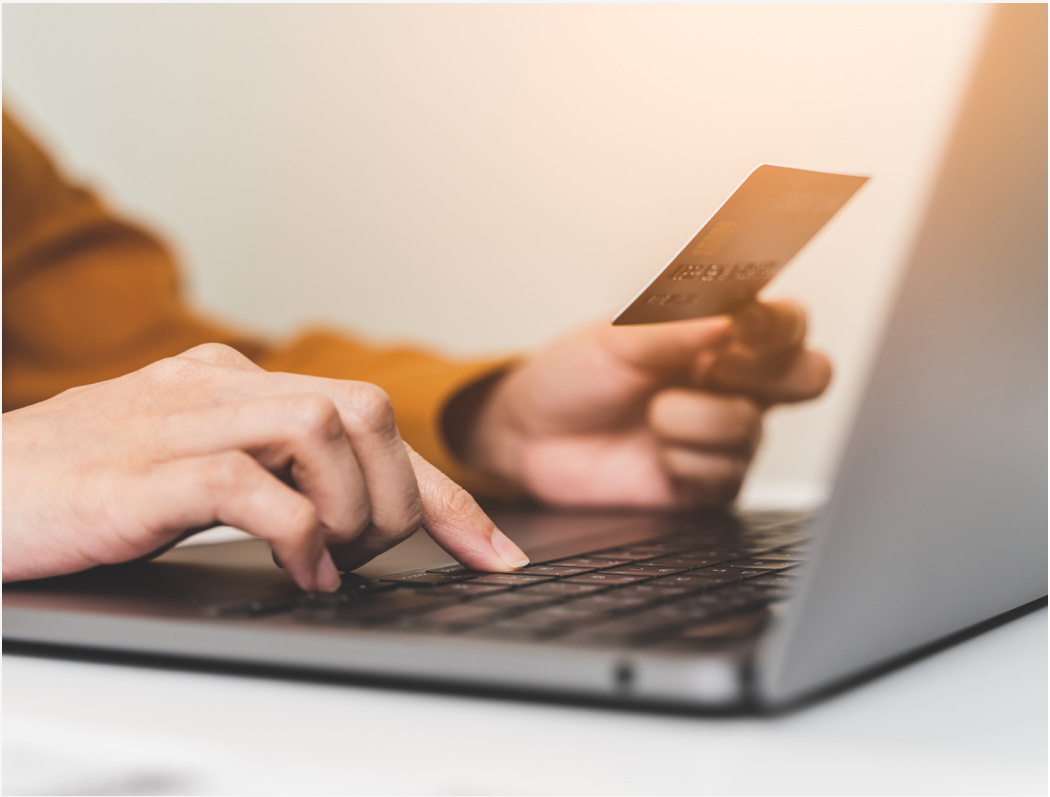
NEXT



# Tips on how to protect yourself from online fraud

NEXT | HELP

Next I Help V.3
Updated 29.09.22

# Simple steps to help you protect yourself from online fraud

## Passwords & Authentication

- To help protect your NEXT account you can now set up 2-factor authentication (2FA). This will provide an additional layer of security to your account requiring more than just a password to login. For further details and how to activate, scan the QR below.

Help protect your account by setting up 2 - Factor Authentication.
**Scan the QR code or visit next.co.uk/account for further details**

Scan me

**A verification code is sent via sms, this feature allows you to set up 2FA to:**

Authenticate every time you log on **OR** only authenticate each time you log in using a different device.

- Change your passwords and pins frequently.
- Do not use the same password on different accounts.
- Use a combination of letters, numbers and symbols when creating a password such a 'F1shD0gCh41r'.
- Create a memorable password that's also hard for someone else to guess, you can combine 3 words together for example (fishdogchair).
- Avoid using predictable passwords like, your name, your family's name, pet names and dates such as your date of birth.
- You can also use a stand alone password manager app to help you create and safely store your passwords.
- If you think your password has been stolen you can use the website **www.haveibeenpwned.com** to check if your information has ever been made public in a major data breach.

## Be aware of scams

- Remember the saying 'If something seems too good to be true, it probably is'.
- Do not give out any personal information to companies or individuals over the phone if they have called you before verifying who they are. If in doubt you can always call them back using a registered number from their website.
- 'Phishing' is the most common technique used to capture your details. It is where a fraudster sends an email or sms that looks authentic, asking you to key in your information (e.g. account number and/or password).
- Next will never ask you to key your email and password unless you are logging into your account online.

## Report it

- If you believe you have been a victim of fraud you should report it immediately. You can contact Action Fraud (see overleaf for contact details) to report fraud and find help and support.
- Contact your bank, or the payment provider if you notice any unusual activity.
- If you have not received your normal statements, contact the company.
- If you receive an email about a change in your account details or for an order you have not requested contact the company in question
- If your cards have been lost or stolen, cancel them immediately.

## Protecting your personal details

- Shred or destroy all unwanted personal documents that hold your personal data, such as utility bills, statements and marketing mailing.
- Secure all your personal documents/information such as passports, driver's licence, birth certificates and statements.
- Check your credit file to see if any unauthorised applications have been created without your consent.
- Check your credit/debit card/Store accounts regularly for any unusual activity.
- If you are going to or recently have moved, request your mail to be redirected (this service is only available for mail sent via Royal Mail).
- Close all inactive accounts. You can also request to be removed from marketing mailing lists.

## Expert support (Full list of contact details found overleaf)

- Registering your details on CIFAS. CIFAS is the UK's Leading fraud preventiondatabase. They are a non profit organisation and serve their members by facilitating the sharing of fraud risk data to reduce the exposure to fraud and financial crime. CIFAS also offers individuals protection against identity fraud.
- There are well established companies such as Equifax, Experian and Transunion who can alert you to activity that may indicate attempted fraud using your name, as apart of an application for credit. Clearscore is also a great tool to use and is free to join, Clearscore provides free credits scores and reports.
- The National Cyber Security Centre is a useful tool to use. The website provides you all the advice and guidance you will need to protect yourself from online fraud, and what to do if you have been a victim of fraud.
- For extra protection you can often register through your card provider for additional levels of security such as a 'verified by visa' 'mastercard securecode' and 'Amex SafeKey'. All future transactions will require you to verify your identity.

# Useful contacts

### NEXT ACCOUNT INVESTIGATION TEAM

**Tel:** 0333 777 8901

**Email:** customer_team@next.co.uk

### ACTION FRAUD

**Tel:** 0300 123 2040

**Web:** www.actionfraud.police.uk

### NATIONAL CYBER SECURITY CENTRE

**Web:** www.ncsc.gov.uk

### CIFAS

**Web:** www.cifas.org.uk

### EXPERIAN

The Sir John Peace Building
Experian Way
NG2 Business Park
Nottingham
NG80 1ZZ

**Tel:** 0344 481 8000

**Web:** www.experian.co.uk

### EQUIFAX CREDIT FILE ADVICE CENTRE

P.O. Box 10036
Leicester
LE3 4FS

**Tel:** 0800 014 2955 **OR**
0333 321 4043

**Web:** www.equifax.co.uk

### TRANSUNION UK

One Park Lane
Leeds
LS3 1EP

**Tel:** 0330 024 7574

**Web:** www.callcredit.co.uk

### CLEARSCORE

1-45 Durham Street
Vauxhall
London
SE11 5JH

**Tel:** 02075828212

**Web:** www.clearscore.com

### ROYAL MAIL REDIRECTION

**Tel:** 0345 777 7888

**Web:** www.royalmail.com/personal
receiving-mail/redirection

NEXT