Keeping yourself cyber safe at home, online and on the move

At Fidelity, cybersecurity is a crucial part of how we operate our business. However, in an increasingly digital and online world, it's just as important that information and data is secured and protected in our personal lives too. The best way to ensure we stay safe online is to be aware of threats and know how to counter them. To that end, this guide contains ten simple and effective tips designed to help you stay 'cyber safe' wherever you may be.

Fidelity INTERNATIONAL

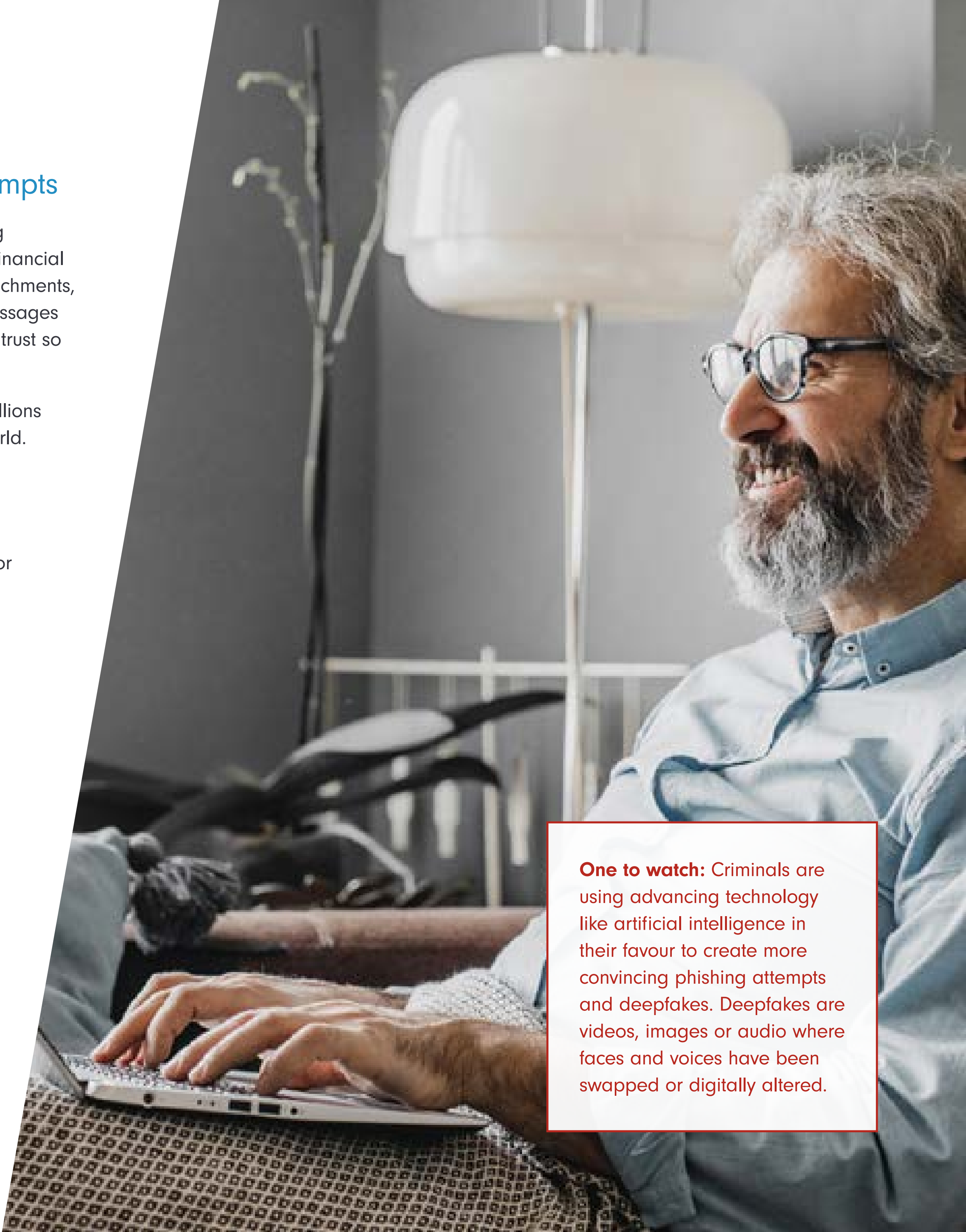
1 Be on the lookout for social engineering attempts

Social engineering is the practice of manipulating someone into doing something that compromises their security, usually for the purpose of financial gain. It can take many forms but can include phishing emails with attachments, which if opened download malicious software on your device, text messages with links to fraudulent websites or phone calls which aim to establish trust so you willingly provide sensitive information like your password.

The most common form of social engineering is phishing. Everyday millions of phishing emails are sent out to unsuspecting victims all over the world. But how can you tell a real email from a scam one? Here are a few pointers:

- Look out for requests which use emotions to get reactions. If you receive something which is unexpected, makes you feel something or asks you to take action – slow down and think carefully.
- The message asks for personal information, such as passwords, or has links to sites requesting your log-in details.
- You're not expecting anything from the sender or there's surprising news (such as winning a competition you didn't enter).
- The email says you must act now to avoid losing money or having your account access cut off (scammers often try to get you to act quickly without thinking).
- The URL (the sender's address) looks odd, is spelt incorrectly, or doesn't match previous examples.
- Something just seems wrong – trust your intuition and common-sense judgment erring on the side of caution. Be safe, not sorry.

Scams can come in many forms and could combine methods such as text message with phone calls to make them more believable. Be suspicious and follow the 'trust but verify' approach before you take an action.



One to watch: Criminals are using advancing technology like artificial intelligence in their favour to create more convincing phishing attempts and deepfakes. Deepfakes are videos, images or audio where faces and voices have been swapped or digitally altered.

2 Beware of email hacking!

Never transfer money on the basis of an email alone
Unfortunately, email is a favoured channel for cybercriminals and email hacking – the taking over of someone's account without their knowledge – is becoming much more prevalent and is now a common feature of financial fraud. You may think you have received an email from a trusted source, such as your financial adviser, but you could have received a message from a criminal who has taken control of their email account.

Always apply the 'trust but verify principle' – it is particularly important you double check with the sender before transferring any money which has been requested by email. Don't check by replying to the email you've received – you may be communicating with the fraudster – always call and speak to the individual or organisation personally to make sure the request is genuine.

3 Protect your accounts

Passwords are an obvious way to prevent unauthorised access to accounts, although they need to be strong, long and unguessable to be effective. Use three random words to create a memorable 'passphrase' and then mix in some symbols and numbers (the longer you make your passphrase the better). Always use a unique passphrase for each account that holds your most sensitive information. This is especially important for your email account as it contains so much personal information and can be used as the gateway to many of your other online accounts.

No matter how strong your passphrase is, there is always a chance it could be hacked or stolen through no fault of your own. Adding multi-factor authentication provides an extra layer of protection by having a site or service verify your identity using two different elements. By using something you know, like a passphrase, and something that only you have, such as a one-time code or fingerprint, you can help secure your email account and other important services.

4 Limit what you store

If your email account becomes your document store, then, if compromised, a hacker could gain access to all of the information you are stockpiling including attachments, photos, contracts, invoices, tax forms, reset password requests for other accounts – sometimes even passwords or credit card PINs!

To minimise risk, only save limited information within your email account. Save any sensitive personal information outside of the mailbox in secure document repositories.

5 Ensure you use a secure wi-fi network

It's easy to stay connected with public wi-fi access points everywhere – in restaurants, coffee shops and shopping centres – but accessibility can come with risk.

Public wi-fi 'hotspots' are exactly that – public – they offer no privacy or protection to your data and communications. Never use public wi-fi to access sensitive information, like your email account, or enter log-in details or credit card information while connected to it.

6 Regularly update your devices

Keeping your operating system and apps up to date is important as the latest updates can contain security upgrades and protection from emerging threats. To be sure you don't miss any important improvements, set updates to happen automatically.

Additionally, make sure your antivirus product is turned on and up to date. Windows and macOS system software have built-in malware protection tools, which are suitable for this purpose, so make sure they are activated.

7 Protect your data with regular backups

Ransomware is becoming increasingly common. This malicious software – which can be downloaded by opening attachments in phishing emails or through following instructions on a fraudulent website – encrypts your data, preventing you from accessing it. The criminals will then make contact demanding a payment (ransom) to restore your access. Please do be aware, reports show there is no guarantee your data will actually be restored, even if you pay in full.

One of the best ways to protect yourself from ransomware is to make regular back ups of your most important files. Many devices have 'auto-backup' options, so make sure these are turned on. Back ups can be made to a cloud backup service, a different device or to removable media such as a USB stick (make sure you know how to restore the files from any backup should you need to do so). Ensure back up devices aren't permanently attached to your computer or they could fall prey to ransomware attacks too.

8 Be careful how you use social media

Social media can be a hugely fun and powerful way to keep in touch with old friends (and make new ones), share interests and keep up to date with the latest trends. Unfortunately, sites like Instagram, TikTok, Facebook, X (formerly Twitter), YouTube, Pinterest and LinkedIn are just as popular with criminals.

Be wary of putting up any information that could provide answers to your security questions, steal your identity, access your accounts or even be used to target you with more enticing phishing emails. Don't share your home address, email address, phone number or date of birth. Manage who can access your posts and your data by regularly reviewing your privacy settings on your social media accounts. Also, try not to let the world know exactly where you are every minute of the day. Telling everyone when you are out and about or away on holiday will also let them know when you're not home.

9 Keep your guard up when you're out and about

If you regularly take your mobile device, tablet, smart phone, or laptop with you when you go out, you need to take digital security just as seriously on the move as you do at home. As well as being easier to lose (or just leave behind), you are taking your device out of the controlled environment of your protected home and personal wi-fi.

One of the simplest and most effective things you can do to protect your data is to take a minute to look through your device's security settings. Using a screen lock, which requires a passcode to deactivate, is vital if you ever become separated from your mobile technology. Turning Bluetooth off when you aren't using it helps prevent hackers from connecting to your device and stealing your data.

Android, Apple's iOS and Windows operating systems all include remote find, lock and wipe features as standard. Make sure you enable and familiarise yourself with these features so you are ready to use them if your device goes missing.

Another useful tip is to record your IMEI (International Mobile Equipment Identity) Number. The IMEI is a 15-digit number that identifies your devices and can be used to block your phone if it's stolen. Dial *#06# on your mobile phone, then screen capture the IMEI number and save a photo of it separate to the device.

10 Knowledge is the best defence

When it comes to your online financial safety, knowledge is one of the best tools you have. Understanding the latest security advice and guidance means you can stay one step ahead of cybercriminals and will help you counter the emerging scams and threats.

How we protect you and your data

Fidelity understands the importance of keeping your information safe and your identity secure. We have a dedicated cyber-defence team and use proven, industry-recognised security tools and processes to protect against fraud and security breaches and we regularly upgrade this protection in response to advances in security threats. Fidelity is a member of Cifas, the UK's fraud prevention agency, which works closely with law enforcement partners. Cifas Protective Registration is a scheme that helps us protect you, should you find yourself at risk of fraud, financial crime or online criminal activity.

If you have any concerns about the security of your Fidelity account, please call us as soon as possible on 0800 358 4060. Please have your Customer Reference Number (CRN) and PIN ready. If you don't have a PIN, you can create one by logging in to your online account.

Additional advice on staying safe online

For more help and advice, simply visit:

- The National Cyber Security Centre
- Stay safe online
- Action Fraud
- Cifas

You should also regularly check haveibeenpwned.com to see if your email account has been compromised.

Important information

Information contained in this document has been obtained by Fidelity from public sources. Care has been taken by the staff of Fidelity in compilation of the data contained herein and in verification of its accuracy when published, however the content of this document could become inaccurate due to factors outside the control of Fidelity and should, therefore, be used as a guide only.

This document is published and distributed on the basis that Fidelity is not responsible for the results of any actions taken on the basis of information contained in it nor for any error in or omission from it. Fidelity expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this document.

Fidelity
INTERNATIONAL

Issued by Financial Administration Services Limited, authorised and regulated by the Financial Conduct Authority. Fidelity, Fidelity International, the Fidelity International logo and F symbol are trademarks of FIL Limited.