Fraud and Cyber awareness Guide

dudley
your Building Society

Online + Dudley

Here at Dudley Building Society we are committed to helping you to protect yourself from fraud and scams and giving you peace of mind as you increase your online activity.

We understand that the prospect of criminals attempting to exploit your online activity can be overwhelming, so we have created this guide to equip you with the knowledge to be fraud and cyber aware and to help you keep your online experience as safe as possible.

Fraud Awareness

You might have heard words such as 'scam', 'con', 'swindle', or 'cheat' as ways to describe fraud, and there are many, many more.

Criminals are specialists in impersonating people, organisations and the police. They may target you, or any of us, in the hope that we'll let our guard down for just one moment. This is all they need to take advantage, for their own financial gain.

You can reduce your vulnerability to this type of crime by being wary of any unsolicited emails, calls and texts asking you for information about your accounts, passwords, logins or other security details.

If you are in any doubt about the validity of any communications you receive, contact the organisation directly, ensuring you do not click on any links, open any attachments or respond to any requests for information or money.

How do you know you are dealing with us?

We take our responsibilities very seriously and we will **never** call, email, text or ask you to do any of the following...

- × Disclose your passwords to your accounts
- × Move your money into another 'safe' account
- × Ask you to make or confirm any payments via email by providing you with a link

Please be vigilant about any messages you receive that claim to be from Dudley Building Society. If you are concerned about anything you receive, it is essential that you contact us before making any transactions or disclosing your personal information.

What else can you do?

Keep your personal information personal - If fraudsters can find out enough information about you they can use this to impersonate you and apply for new accounts or services in your name.

They may also attempt to take over your existing accounts by impersonating you and changing your details.

- Make sure you always dispose of your personal information securely e.g. by shredding it.
- Take care when posting personal information online e.g. on any social media profiles and make sure your profiles are restricted to your 'friends'.
- Monitor your emails regularly; if you receive a notification saying the details on your account with us have changed and it wasn't you that made the change, then tell us immediately.
- Regularly get a copy of your creditfile and check it for entries you don't recognise.

Remember to always

- **Stop** – take a moment to stop and think before parting with your money or information. It could keep you safe.
- **Challenge** – Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect** – Contact your bank or building society immediately if you think you've been scammed and report it to Action Fraud at actionfraud.police.uk or on 0330 123 2040.

What do I do if I think I've been the victim of a fraud or a scam?

Stop any transactions – if you have made any transactions, contact your bank or building society as soon as you can. They may be able to stop or reverse any payments.

Report it – you can make a report to the Police Action Fraud line by calling:

0300 123 2040

dudley your Building Society

For more information on how you can prevent falling victim to fraud or a scam, including advice on how to report any suspicious activities, please visit the dedicated fraud awareness page on our website dudleybuildingsociety.co.uk/fraud-awareness/

Cyber awareness

Keeping your data safe is our number one priority at the Society, but there are also some steps you can take yourself in your day-to-day life.

Password Security

Create strong and unique passwords. When setting up passwords, remember to make them as unique as possible. Even though you might be tempted, please do not reuse passwords that you are already using on other websites on the internet. Also, enable two-factor authentication (2FA) wherever possible.

Use Anti-malware or Anti-Virus

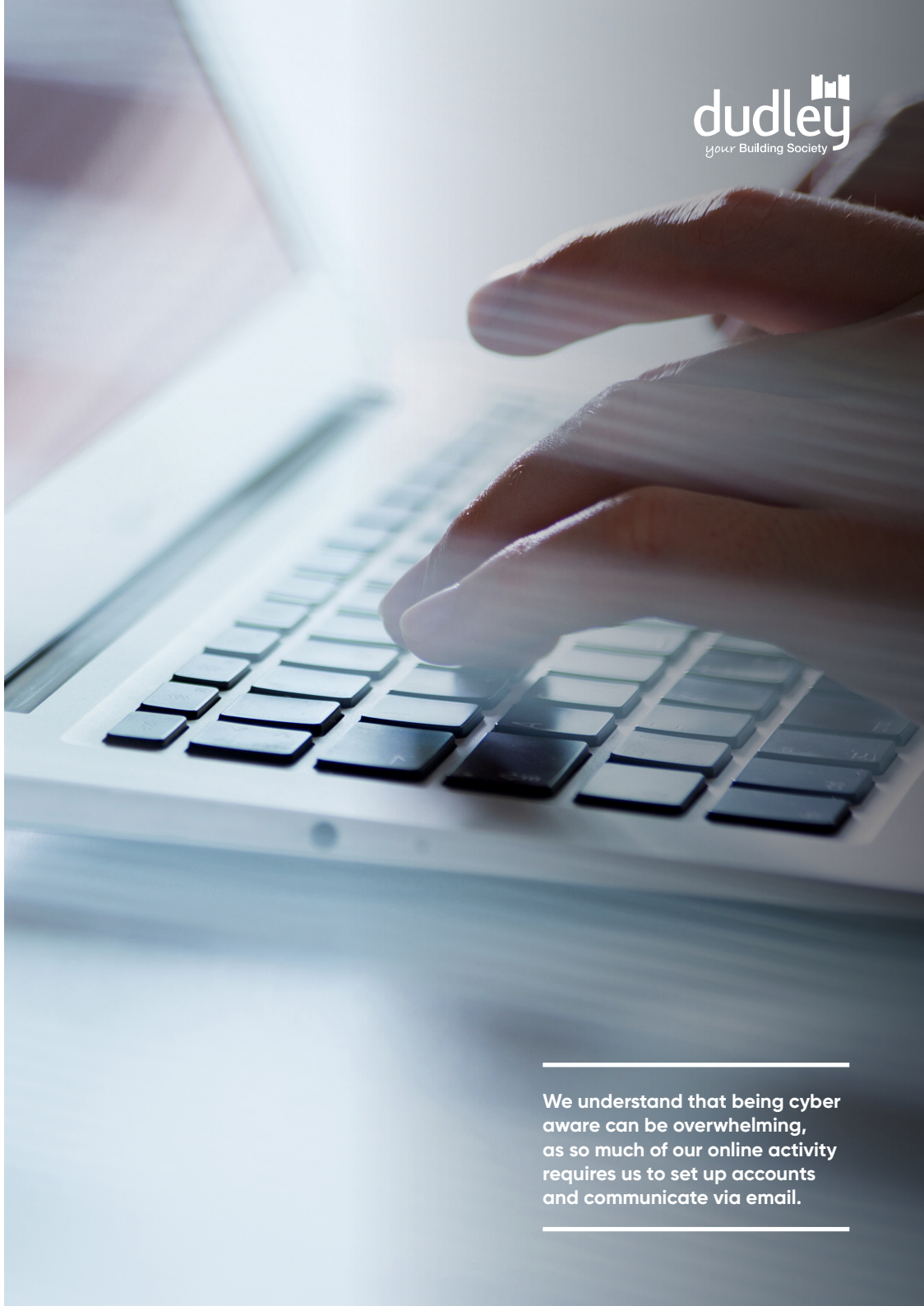
Protect your device by using an Antivirus software (AV). There are several AV devices in the market, which can be downloaded and installed very quickly. If you're unsure on which one to use, then simply search the internet and read the reviews to help you make a decision.

Update, update, update, update...

Ensure you regularly update your mobile phone, computer, or tablet. Typically, updates need to be done monthly, however there might be some urgent updates sent on an ad-hoc basis. Ensuring you check for regular updates will help protect your operating system against security threats such as viruses.

Only use secure websites

Check that every website you visit has 'HTTPS' in the address. This is easy to check. All you need to do is make sure the site you are visiting has HTTPS at the beginning of the address and not just HTTP (without the 'S'). The 'S' stands for secure so this should be easy to remember. For example, the URL should look like this: **https://www.example.co.uk.** You'll usually see a padlock icon too, showing that the site is secure.



dudley your Building Society

We understand that being cyber aware can be overwhelming, as so much of our online activity requires us to set up accounts and communicate via email.

Suspicious emails

Criminals increasingly attempt to exploit individuals through phishing emails, which attempt to obtain sensitive information such as usernames, passwords, and bank account details. They will often do this by impersonating a genuine organisation which you may already have accounts with such as banks/building societies, social media sites and shopping sites.

How does this work?

Criminals are known to clone websites or make similar looking websites, using company logos and details to make the website look authentic. The website is then used as part of the 'Phishing Campaign'.

There are a variety of things that you should look out for in an email which may indicate it is suspicious.

Email address

Does the email address look like it's from the correct sender, check for any small spelling mistakes that may indicate this is not a legitimate email address.

Spelling and grammar

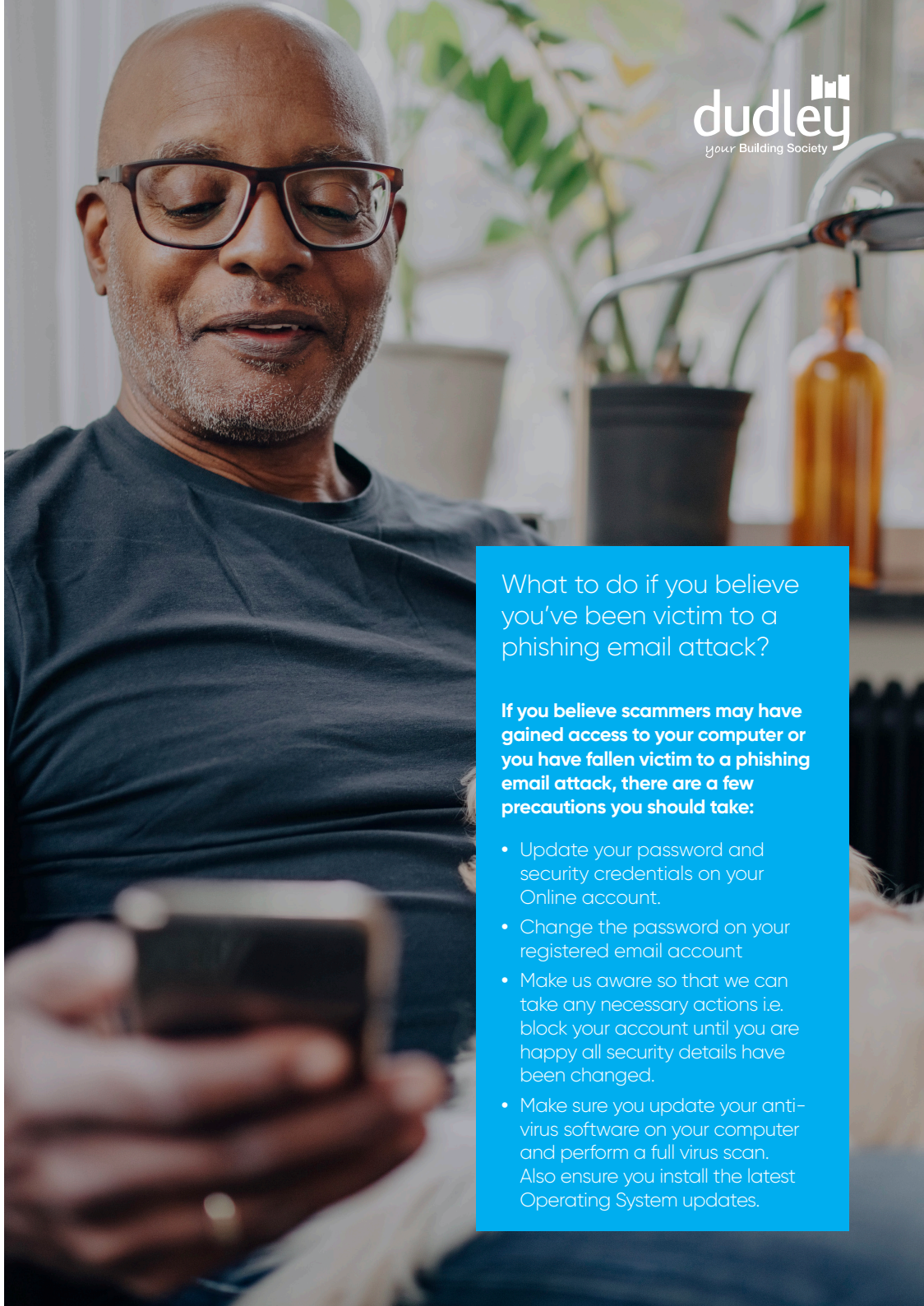
Spelling and grammar mistakes can often indicate that the email is suspicious.

Lack of professionalism

Phishing emails will often be worded in an unprofessional way, either in a very casual or panic inducing tone. e.g. act now or your account will be blocked.

External links and email attachments

Emails that encourage the recipient to click through to links/attachments for verification or further information could be suspicious.



What to do if you believe you've been victim to a phishing email attack?

If you believe scammers may have gained access to your computer or you have fallen victim to a phishing email attack, there are a few precautions you should take:

- Update your password and security credentials on your Online account.
- Change the password on your registered email account
- Make us aware so that we can take any necessary actions i.e. block your account until you are happy all security details have been changed.
- Make sure you update your anti-virus software on your computer and perform a full virus scan. Also ensure you install the latest Operating System updates.

Our Emails

If you do receive an email which appears to be from us and you suspect it could be a phishing email, please do not click on the links within the email and always open a separate Internet browser session and browse to our website independently.

Please report any suspected phishing emails to **phishing@dudleybuildingsociety.co.uk**

Our email notifications will always come from the addresses below:

noreply@dudleybuildingsociety.co.uk
marketing@dudleybuildingsociety.co.uk

Any emails that are received from an alternate address will most likely be fake, therefore please delete and call us to verify if in doubt.

The example email opposite contains our legitimate logo and Head Office address, and attackers will make use of easily accessible content to trick customers. The look and feel will be a close match so ensure you check, double-check, and triple-check!

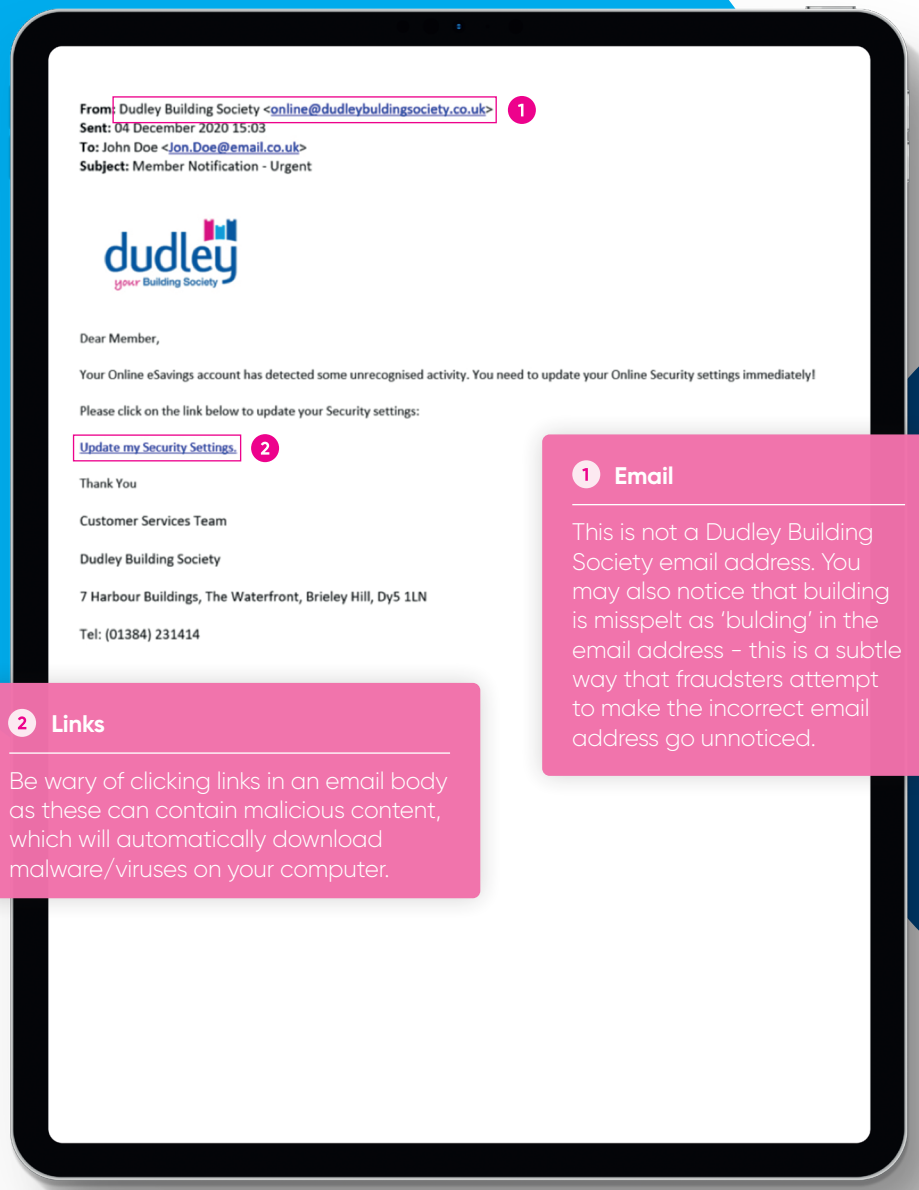
If you are ever in any doubt that an email is suspicious, always contact the relevant organisation directly to confirm whether it is legitimate, ensuring you do not click on any links as this is often the way that criminals gain access to your personal information.

Top tip

Hackers will aim to cause panic to try to make you react quickly, which in this example is to 'click the link' and 'update your security settings' as fast as possible.

Always try to remain calm and access your account by opening a new internet browser session and browsing to the URL

connect.dudleybuildingsocietyonline.co.uk



Keeping your Online Service secure

Your Online Service has been designed with the security of your personal information at the forefront. We understand you may be wary of managing your finances online, but we would like to reassure you that we are committed to making your online experience as safe as possible.

Our Login Security

Our Online login process is compliant with the Strong Customer Authentication (SCA) regulation. This regulation requires two out of the three factors opposite to ensure you can verify yourself:

"Something you know"

This is a piece of information that only you know, like your password.

"Something you have"

This is a secure piece of information that is either sent to or generated on a device you own, such as a One-Time Passcode sent to your mobile phone.

"Something you are"

This is something that is unique to you, like your fingerprint or retina scan.

Setting up a strong password

Always choose a unique password and remember to include a combination of: **Uppercase, Lowercase, Numeric and Special Characters**.

Our website will force you to create a password of a specific length, which must contain certain characters.

Please do not share your password with anyone and remember at no point will a member of staff from the Dudley Building Society ask you to disclose your password.

Protect your mobile device from scams and hackers

A lot of organisations including us implement One-Time Passcodes as a security measure, but unfortunately criminals can attempt to exploit a One-Time Passcode with a 'Sim Swap Scam'.

A Sim Swap Scam is when fraudsters get hold of your personal information and convince your mobile service provider that they are you and that 'you' have lost your mobile phone. Their goal is to get the service provider to swap your mobile phone number to a new SIM card that they have in their possession.

Once the number is swapped, they will then start receiving your calls and text messages including any One-Time Passcodes for your online account. SIM Swap Scams are also referred to as SIM Hijacking, SIM attacks, SIM cloning, SIM splitting, SIM porting or SIM port-out.

How can I prevent a SIM swap scam?

Call your mobile service provider and enable a unique password or PIN on your account that must be given to successfully change your mobile number to another SIM card. Simply call you mobile provider and say "I want to add some security controls on my account so that I am protected from a SIM swapping scam"

We recommend that all our online customers follow this advice before opening your online account to ensure you have the adequate protection in place.

dudley your Building Society

Follow us on social media for the latest on what we're up to.

@DudleyBS
Dudley Building Society
Dudley Building Society
dudleybuildingsociety


dudley
your Building Society