Some advice to help protect yourself online

Here are some easy ways to protect yourself online:

Passwords: Make sure that your password and memorable data is a mixture of letters and numbers that cannot easily be guessed. Don't keep a written record of your passwords and remember that legitimate organisations will never ask you for complete passwords over the phone or by email.

Anti-virus software: Install software that protects your computer from viruses and unwanted programs and make sure it is kept up-to-date. Try to scan your computer regularly for viruses.

HTTPS: If you're entering personal information, such as your account number, make sure the website address begins with 'https' and that there's a padlock symbol within the browser as this indicates that a site is secure.

Wireless networks: Avoid using public computers to do your internet banking. When using a wireless router make sure it's password protected and completely secure; never give visitors access to your network.

Emails: We'll never send you an email demanding that you log in to your account immediately or it will be shut-down.

Account details: Never give your account details or other security information to anyone unless you know who they are and why they need them.

Protecting yourself against frauds and scams

Passwords: To help keep your data and personal information safe you should ensure you set a strong password on your account. To help achieve this see the useful points below.

- Don't use personal information
- Don't use easily recognisable numbers
- Avoid using the word 'password'
- Use a mixture of letters and numbers
- Use a mixture of capital and non-capital letters
- Use symbols such as an asterisk or exclamation mark
- Make sure you have a long password
- Modify easy to remember phrases
- Try using three completely random words

It's important that you change your password regularly and use different passwords to those you've already used for other accounts. Also, don't write passwords down or share them.

Keeping your browser up to date: In order to benefit from the latest security features that Google and Microsoft introduce as a matter of course, it is important that your web browser is up to date.

Types of frauds and scams

Phishing: Phishing refers to emails that attempt to fraudulently obtain your sensitive information. These emails will often direct you to a website requesting you to enter your personal information such as bank login details and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Common features of phishing emails are:

- Appear to be too good to be true (they often are)
- Have a sense of urgency
- Address you in an unusual way
- Contain multiple grammatical and/or spelling errors
- Contain hyperlinks or attachments which may be from an unusual sender

If you receive an email from us that you are suspicious about, simply forward the email to enquiries@harpendenbs.co.uk and we will investigate it.

Vishing: Fraudsters can also make unsolicited telephone calls encouraging individuals to provide sensitive data such as personally identifiable information. This is known as Vishing.

If you're unsure about a call you receive from any financial organisation, call them back but from another phone line such as a mobile or landline. We would recommend waiting about five minutes before doing so as sometimes the fraudster on the other end doesn't hang up so when you make another call, they're still on the line.

When we make an outgoing call to a customer, please be aware that we will ask for personal data to identify you. We encourage you to follow the steps above if you are at all suspicious about any aspect of the call.

Furthermore, with online accounts, sometimes scammers will try to get access to your account by using a one-time passcode/password (OTP). They will fill in the website with all the information they have for you like name and/or email for example. They will then call you pretending that they work for the company that you have your account with. Usually, the scammer will explain that they are calling to offer you an incentive such as a bonus or an extra for free in your account.

They will sound believable and they will explain to you that you will now receive an OTP so that they can 'proceed' to verify your account. At that moment the scammers will still be on the website and the website will send you an OTP which they will ask you to read out to them. They will then enter the OTP and gain access to your account.

Pharming: Pharming is another scam whereby a fraudster installs a malicious code on a personal computer or server. This code usually redirects any clicks you make on a website to another fraudulent website without your consent or knowledge.

Be especially careful when entering financial information on a website. Look out for the 's' in https and the key or lock symbol in the browser. Don't click on the website unless you're absolutely certain that the website is secure.

More useful links to protect yourself against frauds and scams

Below are a series of links to useful third party websites with more information about types of frauds and scams, and ways you can avoid falling victim to them;

Take Five
www.takefive-stopfraud.org.uk

Get Safe Online
www.getsafeonline.org

Action Fraud
www.actionfraud.police.uk

Ofcom
www.ofcom.org.uk/online-safety