Fraud Prevention

As an organisation we are seeing and are aware of increasing fraudulent activity and an increase in the number of attempted frauds and threats to security.

There are a number of actions that can be taken to minimise the risk of loss to branches.

Impersonation Fraud

These tend to be emails purporting to be from a known person – perhaps the DC or secretary (whose details are often easily found on the Branch website), asking for immediate payment of an invoice or reimbursement.

They often originate from abroad and are easy to spot as English is not the first language of the scammer.

Increasingly these scammers are using Artificial Intelligence to create emails in the style of the person they are impersonating and are becoming more difficult to spot.

If in any doubt, contact the person who has 'sent' the email and suggest that they change their password as it is likely that they have been hacked.

If you press reply, you can see the email address that it is going to send back to. Check that this is the person's real email address.

Online Purchases

When purchasing goods or services online from companies you have dealt with previously be aware of

Changes to account details – telephone numbers / personnel / bank details

Changes to email addresses

Compromised email addresses – where the email address is very similar to one you are expecting to see but maybe an extra character has been added to the email address.

All of these can indicate that the company you are dealing with has been hacked.

If in any doubt, ring on a known number to check with a person that you know is a bona fide employee of the organisation.

Credit card purchases offer more protection than debit card transactions, however branches are not allowed to hold credit cards.

Remote Access Scams

Usually originating from a phone call, purporting to be from a Bank, the Police, Action Fraud, Microsoft Technical Support the scammer tries to convince you that there is an urgent issue with your account and that they need you to download software so that they can prevent your money being stolen. They will try to put you under pressure to download software which will allow then to fix the issue remotely.

If you install this software, it will load a fake screen on your device whilst in the background, they are actually compromising your account, and transferring your money to another account where it quickly is moved on. Approximately 95% of these scams ask you to download Any Desk or Team Viewer.

Terminate the call and contact your bank's fraud team. They will investigate and put a marker on your account – this will not affect your credit rating but will allow the Credit Referencing Agency to put a marker on the account to show that it has been subject to attempted fraud.

Overpayment Scam

A cheque is paid to you and is for an amount exceeding that due. The sender then asks for a refund of the difference but before the cheque clears, they cancel the cheque.

There are also similar incidences of Paypal transactions.

If this happens, wait until the payment to you clears before you issue a refund.

Online Retail Scam

Purchases made to fake websites, where the goods don't exist.

Credit card purchases offer more protection than debit card transactions, however branches are not allowed to hold credit cards.

If you are purchasing from a new supplier, check the website carefully and google the company to see if there are reported scams and / or independent reviews.

Barclays have explained to us that 98 % of the scams that they deal with fall into the above categories.

If you feel under pressure or are told that there will be consequences if you do not act – step back and think before you act and contact a trusted person at the company or your bank on a number, you have used previously or have found on their main website.

Cyber Security

Cyber-attacks rely on the ability of the scammer to use your data to impersonate you on websites.

Many people use the same or similar passwords for multiple sites.

Most of these attacks fall into one of 3 categories.

Data Breach

Breaking your password and finding more details from your account – such as your DOB will allow access to your online account and hackers can then impersonate you and change the destination of your regular payment.

The website 'HaveIbeen pwned.com' allows you to enter your email address to see if your email account has been breached.

3 Steps to better security

Step1. Protect yourself using 1Password to generate and save strong passwords for each website .

Step2. Enable 2 Factor authentication and store the codes inside your 1password account.

Step3. Subscribe to notification for other breaches and then just change that unique password.

You can't stop a data breach from happening but using different passwords everywhere can greatly minimize their impact. With Password1, you don't have to remember all your passwords, and it integrates with Have I Been Pwned to monitor your logins so you can take immediate action.

Brute Force

Guessing your password.

Offshore hackers set up computers which can mine for passwords.

Rockyouwordlist lists over 14.5 million passwords which were breached in less than one minute.

You can enter your password(s) into HaveIbeen pwned.com to see if it has been identified as a Breached password.

Current advice is to use 3 random words for a strong password (Pass phrase). These are harder to crack as the combination of letters is so much longer and the permutations are greater.

You can check how secure your password is and how long it might take a computer to guess it using a website such as 'how secure is my password'.

The results might surprise you.

A password such as 'Kitten_oak_feeder' would take a computer 8 trillion years to guess.

Conversely a one-word password with random numbers 'Kitten321' would take only 3 days.

And 'Kitten' would take 4hundred milliseconds.

Social Engineering / Phishing Scams

These are emails purporting to be from a genuine company. When you click the link in the email to log in it takes you to a fake site, whereupon malicious software is downloaded.

Often the email says, ‘we were unable to take your latest payment’.

These emails are opportunist so can impersonate companies that you know you don’t deal with – in which case you should block the sender and delete the email.

You can take steps to minimise your risk from these attacks by

Hovering over the ‘from’ email address as often this is obviously a scammer.

Check that the email is personalised -not ‘dear customer’.

Copy the link by ‘right clicking’ it and copying it into a website such as Virus Total to scan the link for malicious software.

Open a new tab on your browser and manually type the address on the link into that browser. Log in to your account using this tab and then return to the original email. If you are on a genuine site because you are already logged into the website, you will not be asked to log in again.

In all cases of Cyber fraud, it is important to be vigilant and if you are unsure do not click links and change passwords frequently.