BEWARE !!

DON'T BECOME A VICTIM OF IDENTITY THEFT OR ONLINE SCAMS

Scottish Business Crime Centre
Working in Partnership for Safer Scottish Commerce

SCDEA

Am I bothered?

Why do I need to be concerned about identity theft? I don't have a lot of money or assets, why would I be a target for identity theft?

Identity theft is one of the fastest growing consumer crimes in the country. Identity thieves don't just steal your money; they steal your name and reputation and use them for their own financial gain, and it can seriously jeopardise your financial future.

Imagine having thousands of pounds of unauthorised debt and a wrecked credit rating because of identity theft. The unfortunate reality of identity theft is that it is you, the victim, who is responsible for cleaning up the mess and re-establishing your good name and credit. The experience of thousands of identity theft victims is that this is a frustrating experience that often requires months and in the worst case scenario can take years to resolve

It is a known fact that:

* A vast number of people receive credit card applications on a daily or weekly basis. Many of these people throw out card applications without destroying them.
* A lot of people rarely, if ever, reconcile their credit card and bank account balances.

All of these factors make everyone potential identity theft victims. You may be surprised to learn how many of your daily activities expose you to this crime. For example:

* Do you use your personal computer for online banking transactions?
* Do you use your personal computer to buy merchandise or purchase tickets for travel, concerts, or other services?
* Do you receive credit card offers in the mail?
* Do you discard these documents instead of shredding them?
* Do you store personal information in your computer?
* Do you use a mobile phone?
* Do you use your National Insurance number for identification?

You probably answered yes to at least one of these questions about daily transactions that you routinely perform. Each of these routine actions places you at risk of being a victim of identity theft because each of them requires you to share personal information such as your bank and credit card account numbers, your Social Security number, or your name, address, and phone number. This is the same personal information that identity thieves use to commit fraud.

What is identity theft?

Identity theft is one of the fastest growing crimes in the United Kingdom and it is estimated that it is costing victims over £1.3 billion annually.

Identity theft occurs when someone else uses your personal identification information without your knowledge or permission to obtain credit cards, get phone products and services, obtain loans and mortgages, get a job, and commit other types of fraudulent or even criminal acts, **in your name**, leaving you responsible for the consequences.

The identity thief uses key pieces of your information such as National Insurance and driver's licence numbers to obtain credit, merchandise and services in your name.

In the time it takes to resolve these issues, there is a chance that you may lose job opportunities and be refused loans for housing, or a car.

Online scams can be just as effective in obtaining information about you in order to commit crime such as phishing and unsolicited emails asking for help.

What is phishing?

Phishing is when criminals use fake e-mails or links to obtain other peoples sensitive details, for example passwords, usernames or bank account details. Usually a compelling reason is given to persuade you to go to their web site or click on a link contained in an e-mail, quite often the e-mail is supposedly from familiar names in the high street like your bank or Credit card company others include online service providers, auction sites etc. The web sites now usually look genuine but are in fact designed to lure people into entering personal details. Once entered the criminal can now gain access to your identity, take money from your bank account or infect your computer with a virus which then allows them to control your system.

Things to look for:

* The e-mail is not sent to your own name but uses generic terms like 'Dear account holder'
* The email states that urgent action is required with a threat for example, 'if you do not act now we will close your account'
* The email contains a link that you do not recognise
* Misspelling contained within the email
* The email address is not the same as the trusted companies website address
* Unexpected e-mails from a company you have no business with.
* When asked to enter personal details there is no padlock sign on screen and the browser window does not show **https://** at the beginning of the web address.

Protecting yourself

* It is recommended that you ensure your browser is up to date
* Avoid risky sites, including supposed investment sites
* NEVER click on an embedded link in an e-mail from an unknown or un-trusted source.
* If your e mail system has it, use spam filters.
* Do not give out your personal details your bank etc will never ask for passwords or security codes online via email. Phone the bank to make sure first.
* Do not leave personal documents for example a bank statement lying around that can be accessed by anyone else
* Do not throw statements etc out in the bin, wait for a year for business reasons then shred the documents using a cross cut shredder.

I've heard of the term Money Mule, what is it?

A money mule is anyone who is recruited by criminals to use their bank account to transfer money from one country to another, usually from where the criminal lives. Normally there is a cash incentive for the mule to offer the use of their bank account.

Mule recruitment:

* Unsolicited e-mails asking for assistance
* Contact via social networking sites
* Fraudulent vacancies on websites posing as legitimate businesses
* Classified adverts in the press and online which look legitimate and can often look quite professional.

Risks:

* **You are breaking the law and could be charged with a criminal offence**
* Your bank account will be suspended
* All of the money involved will be seized back from your account whether or not the money has already been transferred.
* As a convicted fraudulent criminal it will be difficult to gain any credit or even a bank account again.

How to avoid becoming a victim:

* The old saying 'if it looks to good to be true' is entirely relevant here as offers of large amounts of cash for very little work or no prior experience could indicate a fraudulent scheme.
* Always be cautious of overseas offers as it can be difficult to verify identity.
* You should always research any company that offers you a job checking things like address phone numbers etc.

* **NEVER** give your bank details to anyone unless you know and trust them and even then be cautious!

DON'T LET IT HAPPEN TO YOU !